

INDEX

- Abrams v. United States*, 476
- Access:
- codes, 842
 - Digital Divide and, 524–525
 - privacy and, 412
 - wireless attacks and, 753
- Accessdata's Password Recovery Toolkit (PRTK), 370
- Access Device Fraud Act (1984), 42
- Access point (AP), 751, 779
- Accountability, 414–415
- Account misuse detection, 712
- ACLU. *See* American Civil Liberties Union (ACLU)
- ACPA. *See* Anticybersquatting Consumer Protection Act of 1999 (ACPA)
- ADA (American Dental Association), 556
- Adapters, 505, 510
- Adaptive literacy, 518
- Adbusters group, 307–308
- Address translation services, 504
- Adjudication. *See* Criminal justice system
- Ad networks, 426–427, 432
- ADRs. *See* Alternative dispute resolution techniques (ADRs)
- Advanced Encryption Standard (AES), 365, 581
- Affirmative defense, defined, 121
- Afghanistan, 150
- Aftersnapster.com, 71
- Age. *See* Demographic groups and Internet/technology use
- Age Discrimination in Employment Act (1967), 801
- Air Force's Office of Special Investigations (AFOSI), 119
- Air traffic blackout, 129
- Alappat, In re*, 658
- ALCOA case, 632
- Al-Hussayen (*United States of America vs. Sami Omar Al-Hussayen*), 141
- Al-Jazeera, 149
- AllAdvantage.com, 428
- Alta Vista Technology, 69
- Alternative dispute resolution techniques (ADRs), 38–39, 44
- Altus Net, 773
- Amazon.com:
- Associate program, 40
 - denial of service attacks, 26
 - one-click, patent, 12, 494, 658–659
 - participants, 490, 614
- American Arbitration Association (adr.org), 39
- American Bar Association Task Force, 98
- American Civil Liberties Union (ACLU):
- ACLU v. Miller*, 468
 - Ashcroft v. ACLU*, 15, 59, 442
 - challenges to Patriot Act and DHS surveillance/investigation techniques, 165, 166
 - defined, 556
 - Reno v. ACLU*, 13, 14, 58, 59, 265, 447, 641
- American Express, 29, 30
- American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc.*, 32
- American Law Institute (ALI), 325
- American Libraries Association v. Pataki*, 266, 348
- American Library Association v. United States*, 63
- American Management Association (AMA), 419, 421
- American Mobile Satellite (AMSAT), 734
- American National Standards Institute (ANSI) X12N, 541–542, 555, 558
- American Society for Crime Lab Directors/Lab Accreditation Board (ASCLD/LAB), 377
- Americans with Disabilities Act (1990), 801–802
- America Online (AOL):
- America Online, Inc. v. Does*, 268, 272
 - America Online, Inc. v. Hawke*, 254, 268, 272
 - America Online, Inc. v. LCGM, Inc.*, 223
 - anonymity on, 12
 - AOL versus CN Productions, 270
 - domination of, 44
 - employee e-mail and, 796
 - Geoff v. AOL, Inc.*, 19
 - spamming and spammers, 252, 267–268, 270, 276, 284
- Ameritrade, 836
- A&M Music, 232
- Amnesty International, 611
- A&M Records v. Napster*, 6, 71
- Amsan LLC v. Prophet 21 Inc.*, 25
- Analog, defined, 779
- Anonymity/identity on Internet, 457–478
- anonymous domain registrant, 473–477
 - contrarians, 475–477
 - court rulings, 466–468
 - determining identity on the Internet, 460–462
 - Internet anonymity and the law, 468–469
 - mechanics of, 459–460
 - overview/introduction, 457–458, 477

- Anonymity/identity on Internet (*Continued*)
 remailers, 478
 reverence for anonymity in U.S. political tradition, 465–466
 secure socket layer (SSL), 463, 478, 739
 socks server, 478
 subpoenas seeking identity of anonymous speakers, 471–473
 technical solutions, 462–464
 terms defined, 477–478
 wartime, anonymity during, 469–470
- Anonymizers, 464, 705
- Anonymous DSL (digital subscriber line), 464, 477
- Anonymous surfing site, defined, 477
- ANSI X12N, 541–542, 555, 558
- Anticybersquatting Consumer Protection Act of 1999 (ACPA), 8–9, 45
- Antiglobalization/anticapitalism movements, 315
- APEC (Asia Pacific Economic Council), 669, 681, 686–688
- APOP (authenticated post office protocol), 771, 779
- Apparent identity, 459
- Apple, 7, 232, 301, 302
- Applied Info. Mgmt. Co. v. Icart*, 345
- Appropriation, tort of, 411
- Arizona's Roosevelt Dam, 132, 133
- Arms Export Control Act (1978), 650
- Arpanet, 249
- ASCII, 392
- ASEAN (Association of South East Asian Nations), 669, 681, 682–683, 686
- ASEANAPOL, 686
- Ashcroft v. ACLU*, 15, 59, 448
- Ashcroft v. Free Speech Coalition*, 116
- Asia, 11, 193, 605, 639, 607, 820
 cybersquatting, 11
 lack of civil society structures, 605
- Asian Productivity Organization, 530
- Asia Pacific Economic Council (APEC), 669
- Assent/consent, defined, 352
- Association for Interactive Marketing (AIM), 263
- Association of American Physicians and Surgeons (AAPS), 556
- Association of Metropolitan Water Agencies (AMWA), 168
- Asymmetric:
 defined, 587
 response, 150, 172
 warfare, 731–732, 779
- Asynchronous transfer mode (ATM), 779
- Atari Games Corp. v. Nintendo of America, Inc.*, 229
- ATM (asynchronous transfer mode), 779
- ATM withdrawal, sequence diagram, 492
- Atomic Tangerine, 193
- AT&T, 253, 529
- Attack(s). *See* Wireless information warfare (WIW)
- Attack/defense scenario (A/D), 779
- Attacker identification, 772
- Attractors, 597, 598, 622
- At-will employment, 798, 814–816, 824–825
- Australia, 36, 133, 188, 273, 529, 599, 606, 634, 653, 686–688, 820
- Authenticated post office protocol (APOP), 771, 779
- Authentication:
 authorization and, 716
 defined, 510, 587
 electronic transactions security and, 843
 services, 503
- Authenticity:
 certificates of, 652
 defined, 322
- Automated transactions, 327
- Availability:
 defined, 587
 disruption of, 727 (*see also* Denial of service (DoS) attacks)
 efficient/effective operation and, 834
 e-government security, 568–573
 classes of attacks (physical/logical), 572
 denial of service concerns, 570
 fault-related availability concerns, 568–569
 individual or informally organized hackers, 570–571
 intrinsic availability concerns, 569–570
 logical attacks, 572–573
 nonstate organizations, 571–572
 physical attacks, 572
 sources of denial of service attacks, 570
 state-sponsored attacks, 572
 e-government security mechanisms/techniques for, 578–579
 information assurance and, 748
 wireless information warfare and, 727–732
- Backdoors, 753, 770
- Backups files, 220–221, 838
- Bailey, John, 474
- Ballmer Steve, 310–311
- Bally v. Faber*, 16
- Baltimore Technologies, 331–332
- Bandwidth, communications, 724
- Banks/financial institutions:
 computer security, 487
 Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act), 13, 412, 432, 483
 privacy of records, 412
 terrorism and, 236–237
- Barbie Liberation Organisation, 309
- Barlow, John Perry, 628
- Barnesandnoble.com, 659
- Barron's Online*, 36
- Bateman v. Mnemonics, Inc.*, 229
- BBB Online Privacy Program, 78–79, 429
- BEA Systems, 491, 509
- Behavioral methods, information leak detection, 711
- BellSouth, 246
- Bench trial, defined, 121
- Berube v. Fashion Centre Ltd.*, 799
- BestCrypt, 364
- BGP. *See* Border gateway protocol (BGP)
- Bidder's Edge, 41, 213
- Bill of rights. *See* Constitution of United States
- Biometric security measures, 607, 838, 839
- Bird v. Parsons*, 266
- Black-box testing, 379

INDEX

853

- Black lists, 248, 285
- Blakey v. Continental Airlines*, 26, 800
- Blocking programs, 450–452
- Blogs/bulletin boards, 169, 705, 720
- Blue Cross & Blue Shield of Michigan, 799
- Boeing, 529, 810
- Bombing, Oklahoma City, 105, 572
- “Bomb shelter” legislation (UCITA; Uniform Computer Information Transactions Act), 324, 327, 345, 346–347, 349, 352
- Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, 342
- Booher, Charles, 245
- Border gateway protocol (BGP), 148–150, 172
- Bots/cyberbots, 223–224, 285, 731
- Bounce, 285
- Boureguard, In re*, 658
- Bowers, Harold, 341
- Bowers v. Baystate Technologies, Inc.*, 229, 230, 340, 341, 343
- Boy Scouts, 410
- BPP (business owner’s package policy), 32
- Briggs v. Am. Air Filter Co.*, 217
- Broadband, 520–521, 530–531
- Broker-dealer operations, 27
- Brower v. Gateway 2000, Inc.*, 24
- Browser privacy issues, 422
- Browsewrap agreements, 334–337
- Browsewrap license, 352
- Brussels Convention, 635
- Buckley v. American Constitutional Law Foundation*, 467, 468
- Buffer overflows, 755
- Bunner, Andrew, 16
- Burger King, 7, 8
- Business(es):
 - corporate spying (see Corporate spying)
 - corporate use of personal information, 77–78
 - cyberterrorism and, 158–161, 169–170
 - employee privacy policies, 420–421
 - global e-government and, 609
 - government, compulsory/voluntary cooperation with, 237–238
 - privacy issues for, 419–421
 - terrorism and financial institutions, 236–237
 - USA PATRIOT ACT, and government spying, and, 236–238
 - virus/worm attacks, estimates, 183
 - wiretap laws and, 418–419
- Business-to-business (B2B), 320
- “By any means,” 635
- C4IR (command, control, communications, computers, intelligence, and recognition), 724, 780
- Cable News Network, L.P. v. GoSMS.com, Inc.*, 633
- Caffrey, Aaron, 118–119
- Cairo v. Crossmedia Services*, 23
- Cajunnet, 253
- Cajun spammer. See Scelson, Ronald
- Calder v. Jones*, 35, 632, 633
- California, 16, 17, 30, 35, 116–117, 258, 269, 270, 349, 431, 634, 806, 807
- Callback modems, 838–839
- Caller ID blocking, 482
- Canada:
 - anonymity of juveniles, 26
 - antispam legislation, 280
 - Canadian Human Rights Act, 61
 - Convention on Cyber-Crime treaty, 190, 673
 - copyright law, 66
 - Criminal Code, 185
 - democratic deficit, 608
 - fraudulent wrongful function of computer system, 82
 - free speech, 55
 - Group of 8, 681
 - hate speech, 61
 - Personal Information Protection and Electronic Documents Act, 14
 - privacy, 14, 73, 820
 - Royal Canadian Mounted Police, Tech Crime Unit, 188
 - voting rights, 85
- Canexus.com, 72
- CAN-SPAM Act. See Spam; federal CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003)
- Cantrell v. Forest City Publishing Co.*, 411
- Carbon Defenders League, 308
- Carnivore, 465, 166, 418, 470, 647, 648
- CART (Computer Analysis and Response Team), FBI, 393
- Carpis, J. T., 136
- Caspi v. Microsoft Network*, 338
- Cato, 465
- CAUCE. See Coalition Against Unsolicited Commercial E-mail (CAUCE)
- Caveat emptor, 347–348
- CCIPS (Computer Crime and Intellectual Property Section), 187
- CDA. See Communications Decency Act of 1996 (CDA)
- CDMA. See Code division multiple access (CDMA)
- Cells, 736
- Cellular digital packet data (CDPD), 739, 779
- Cellular phones, 500, 779
- Censorship, 437–453
 - circumstantial, 438
 - content filtering, 453
 - defining, 438–439, 453
 - First Amendment and, 439–441
 - government, 447–450
 - harmful forms of speech, 441–443
 - hate speech, 453
 - overview/introduction, 14–17, 437–438, 452–453
 - “points of control” and, 445–447
 - pornography, 453
 - private, 450–452
 - proxy server, 453
 - security and, 445–447
 - spam and, 453 (see also Spam)
 - tools of the censors, 443–444
- Centers for Medicare and Medicaid Services (CMS), 556
- Central Intelligence Agency (CIA), 187
- Certificate of authenticity, 652
- Certificate revocation lists (CRLs), 580

- Certification and accreditation, e-government, 585–586
- Certification program, I-ACERT security, 158
- Certification service, 503
- CFAA. *See* Computer Fraud and Abuse Act of 1986 (CFAA)
- CGL (commercial general liability) insurance policies, 31–33
- Challenge response mechanism, 767
- Chaos Computer Club, 301
- Chechen resistance, 612
- Chief Privacy Officers (CPOs), 428–429
- Child/children:
 - free speech, 56–59
 - pornography, 56–59, 116
 - privacy, 412–413
- Child Online Protection Act of 1998 (COPA), 15, 59, 447–448, 641
- Children's Internet Protection Act of 2000 (CIPA), 15, 63, 448, 641
- Children's Online Privacy Protection Act of 1998 (COPPA), 13, 412–413, 430–431, 432
- Children's Partnership, 519
- China, 10, 186, 279–280, 443, 445, 449, 525, 527, 651
- CHIP (Computer Hacking and Intellectual Property), 187
- Choice, privacy and, 412
- Choice of evils defense, 109
- CI (counterintelligence), 780
- CIA (confidentiality, integrity, availability), 748–749
- Circumstantial censorship, 438
- Cisco, 529, 775
- CISG (UN Contracts for the International Sale of Goods), 36
- Citizens without borders, 613–614
- Civil justice system versus criminal justice system, 96–97
- Civil Rights Act (1964), 801
- Civil Society gatherings, 612
- Clarke, Richard, 132, 134, 151, 152, 159, 170, 171
- Clean rooms:
 - leakage prevention, 714
 - reverse engineering, 341
- “Click” contracts, 18–19
- ClickNSettle.com, 39
- Click-throughs, 273
- Clickwrap agreements, 24, 45, 47, 334–337, 352
- Clinger-Cohen Act, 584
- Clinton administration/Bill Clinton, 138, 187, 448, 514, 519, 628, 650
- Clipper Chip, 651
- Clustering and network load balancing, 775
- CMS (Centers for Medicare and Medicaid Services), 556
- CMS (Content Management Server), 774
- CNN, 26, 40, 152, 153, 158, 251
- Coalition Against Unsolicited Commercial E-mail (CAUCE), 252
- Code, 444, 453
- Code division multiple access (CDMA), 739, 780
- Code Red worm, 33
- Code walk-through, 401
- Collection limitation, 413
- Colleges/universities, cyberterrorism and, 168–169
- Collin, Barry C., 129–130, 133, 134, 148, 159
- Colorado, 467
- Colorado Regional Computer Forensic Laboratory, 398
- Columbia Insurance Inc. v. Seescandy.com*, 473
- Columbia University's question-and-answer site, 448
- Comb v. PayPal, Inc.*, 340
- Comity, 689, 691
- Commerce Department (DOC), 650
- Commercial off-the-shelf (COTS), 579–580, 725, 780
- Common law:
 - defined, 239
 - fiduciary duty, 211–213
 - privacy, 410–411
 - proprietary rights and trade secrets, 210–211
 - remedies and approaches, 209–216
 - terms of use, 214–216
 - torts:
 - appropriation, 411
 - disclosure, 411
 - false light, 411
 - intrusion, 411
 - trespass, 213–214
- Commons, tragedy of the, 602
- Common Sense* (Paine), 465
- Communication. Assistance for Law Enforcement Act (CALEA), 469
- Communications bandwidth and data-flow rates, 724
- Communications Decency Act of 1996 (CDA), 13, 14, 45, 58–59, 447, 641
- Communications-Electronics Security Group, UK, 599
- Communications equipment, information leakage and, 704
- Communications security (COMSEC), 749, 780
- Communist Manifesto*, 313
- Community, defined, 498, 510
- Community technology centers (CTCs), 528–529, 531
- Compact Flash, 540
- Compaq, 69
- Compartment diffusion, 698
- Complex adaptive systems, 597, 621, 622
- Comprehensive security system. *See* Security system, guidelines for comprehensive
- COMPUSEC, 749
- CompuServe:
 - anonymity and, 12
 - Blakey v. Cont'l Airlines, Inc.* and, 800
 - CompuServe, Inc. v. Patterson*, 338
 - CompuServe v. Cyber Promotions, Inc.*, 265, 268, 452
 - German subsidiary, 445
- Computer Analysis and Response Team (CART), FBI, 393
- Computer crime, defining scope of, 671–672
- Computer Crime and Fraud Act, 82
- Computer Emergency Response Team (CERT), 843–844
- Computer forensics:
 - defined, 825
 - monitoring of employees and, 811–812
- Computer Fraud and Abuse Act of 1986 (CFAA), 187, 215, 221–225, 230, 239

INDEX

855

- Computer security, 81–84
 - COMPUSEC, 780
 - guidelines (*see* Security system, guidelines for comprehensive)
 - legal protection of, 82
 - moral legitimacy of rights of, 82–83
 - threats, defined, 199
- Computer software/hardware manufacturer liabilities, 24–25
- Computer virus. *See* Viruses/worms/malware
- COMSEC, 749, 780
- Con artists, 461
- Condor, The (Mitnick), 100, 145
- Conferences, cyberterrorism and, 167–168
- Confidentiality:
 - CIA factors, 780
 - cryptographic mechanisms, 582–583
 - database design, 583
 - defensive information operations, 749
 - defined, 587, 780
 - disability and medical issues, 801–802
 - e-government and, 576–578
 - electronic transactions security, 842
 - employee records, and e-mail policy, 821
 - impacts on operations, 577–578
 - impacts or consequences of unauthorized exposure, 577
 - legal issues, 578
 - loss of confidence in institutions and service delivery mechanisms, 577
 - mechanisms and techniques, 581–582
 - versus privacy, 576–577
 - protocol and operating system mechanisms, 582
 - threats to, 577
- Configuration management, 755–756
- Connectivity, Digital Divide and, 524
- Consequentialism, defined, 91
- Console cowboys, 304
- Constitution of United States:
 - 1st Amendment, 16, 37, 55, 61, 73, 252, 409, 410, 439–441, 448, 466, 471, 473, 476, 477
 - 4th Amendment, 111, 409
 - 5th Amendment, 104, 105, 409
 - 6th Amendment, 102, 103, 105, 119
 - 14th Amendment, 409
 - e-mail/Internet use policies, and restrictions based on, 807
 - Full Faith and Credit Clause, 637
 - privacy and, 408–410
 - Supremacy Clause, 342
- Consumer(s):
 - digital id and, 494–495
 - online contracts and, 347–349
 - privacy and, 421–427
 - ad networks, 426–427
 - browsers, 422
 - cookies, 424–425
 - IP addresses and browser data, 423–424
 - Web bugs, 425–426
- Consumer Sentinel site, 17
- Content:
 - ability to create, demographic statistics, 519, 520
 - attacks, 746
 - filtering, 453
 - offenses related to, 678–679
- Content Management Server (CMS), 774
- Continental Airlines, 26, 800
- Contract(s), 319–353
 - assent/consent, 352
 - best practice for online contracts, 349–351
 - browsewrap license, 352
 - clickwrap license, 352
 - computer information products, as “good” versus “license,” 344–345
 - consumer protection online, 347–349
 - caveat emptor, 347–348
 - choice of law, 348–349
 - data sharing permissions and, 500–502
 - data structure as, 501, 502
 - defined, 239, 352, 510, 825
 - enforceability of online contracts, 334–340
 - characterizing shrink-, click-, and browsewrap agreements, 334
 - contracts voidable for unconscionability, 339–340
 - manifesting assent to clickwrap and browsewrap agreements, 334–337
 - notice of unusual or onerous terms, 337–338
 - legal concerns, employee e-mail policies, 798–799
 - legal framework for electronic contracting, 324–333 (*see also* Electronic/digital signatures)
 - automated transactions, 327
 - consumer consent, 328–329
 - electronic signatures, 330–333
 - formation and validation of electronic contracts, 325–326
 - notice and consent requirements, 328
 - record accessibility requirements, 332–333
 - record retention requirements, 333
 - signature requirements, 329–330
 - UN model law on electronic commerce, 324
 - U.S. laws covering electronic transactions, 324–325
 - when is an electronic record sent or received?, 326–327
 - maintaining security of electronic transactions, 322–323
 - party authentication and message integrity, 322–323
 - problems concerning authenticity and integrity of electronic documents, 322
 - model clauses, 646–647
 - overview/introduction, 18–19, 319–322, 351–352
 - sale of goods law, and digital information transactions, 344–347
 - software use, 340–344
 - terms defined, 352–353
 - validity, 352
 - warranties, 345–347
 - XNS’s digital identity infrastructure and privacy and, 501
- Convention on Cyber-Crime, 676–680
 - computer-related offenses, 677–678
 - content-related offenses, 678–679
 - copyright infringement, 679
 - Council of Europe, defined, 122
 - countries signing, 121, 190
 - defined, 199
 - jurisdiction, 679
 - procedural powers, 679–680

- Convergence of physical/virtual worlds, 144–145
- Cookies, 77–78, 91, 424–425, 432
- COPA. *See* Child Online Protection Act of 1998 (COPA)
- COPPA. *See* Children's Online Privacy Protection Act of 1998 (COPPA)
- Copyright law:
- definitions, 91, 116, 352, 825
 - employee e-mail/Internet use policies and, 810
 - fair use exception, 4, 7, 22, 46, 66, 229–230, 340–344, 353, 826
 - illicit copying over Internet, 70–71
 - infringement, and global law enforcement, 679
 - musicians, and mass-copy technology, 4
 - online contracts and, 340–344
 - overview/introduction, 5–7
 - reverse engineering and, 340–344
 - willingness of online users to infringe, 68
- Cordless phones, 736, 780
- Corinthian Pharmaceutical Systems v. Lederle Labs*, 327
- Corinthians (Brazilian soccer team), 10
- Corporate sector. *See* Business(es)
- Corporate spying, 205–240
- common law, defined, 239
 - common law remedies and approaches, 209–216
- Computer Fraud and Abuse Act (CFAA), 221–225
- contract, defined, 239
- Digital Millennium Copyright Act of 1998 (DMCA), 227–233 (*see also* Digital Millennium Copyright Act of 1998 (DMCA))
- circumventing technology measures, 227–228
 - defined, 239
 - exceptions to prohibitions on technology circumvention, 229–231
 - fair use and reverse engineering, 229–230
 - impact of recent RIAA and other litigation, 231–233
- Economic Espionage Act of 1996, 225–227
- Electronic Communications Privacy Act (ECPA), 240
- fiduciary duty, 211–213, 240
- government spying and businesses, 236–238
- individuals and, 233–236
- multinationals, 226–227
- overview/introduction, 205–208, 238–239
- PATRIOT Act (*see* USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism))
- series of questions and a hypothetical, 208–209
- Stored Communications Act (SCA), 219–221
- terms defined, 239–240
- terms of use, 214–216, 240
- trade secrets/proprietary rights, 210–211, 225–226, 240
- trespass, 213–214, 240
- Wiretap Act, 216–219
- Corruption of integrity, 728
- Costa Rica, 525
- COTS (commercial off-the-shelf), 579–580, 725, 780
- Council of Europe (CoE), 122. *See also* Convention on Cyber-Crime
- Coupland, Douglas (*Microserfs*), 299, 302, 303
- Covered entities (CE), 539
- Covered writing. *See* Steganography
- Covering tracks (wireless attacks), 753
- Covisint cyberventure, 44
- CPA Web Trust, 429
- Crack, 371
- Crackers, 26–27, 298
- Cracking passwords, 368–371
- Crawlers, 40–41
- Creative Commons project, 613
- Credential sharing, information leakage and, 705–706
- Credit card theft/fraud, 29, 169, 182
- Credit ratings, identity theft, 486
- Credit reports, 412
- Cressey, Roger, 131
- Criminal activity:
- Internet/computer-related (*see* Cybercrime)
 - preventing employees from engaging in, 809–810
- Criminal justice system, 95–123. *See also* Evidence, digital; Jurisdiction
- adjudication, 103–105
 - versus civil justice system, 96–97
 - copyright law, 116
 - cybercrime and, 115–121
 - defense attorney role, 102–103
 - defenses, 105–110, 117–119
 - affirmative, 105, 106
 - failure of proof, 105–106
 - back back, 110–111
 - evidentiary issues, 111–113 (*see also* Evidence, digital)
 - federal cybercrime law, 115–116
 - institutional structure, 97–114
 - overlapping laws, 97
 - overview/introduction, 95–96, 121
 - prosecutor role, 98–102
 - sentencing, 113–114
 - state cybercrime law, 116–117
 - state/federal systems, 114–115
 - terms defined, 121–123
- Crispi v. The Microsoft Network*, 19
- Critical Art Ensemble (CAE), 303
- Critical Infrastructure Protection Project (CIP), 168
- CRLs (certificate revocation lists), 580
- Crossmedia Services (CMS) forum, 23
- Cross-site scripting (XSS), 762, 763, 774, 780–781
- Cryptanalysis, 781
- Cryptographic attacks, 747–748
- Cryptographic mechanisms, 580–581
- Cryptography, 587, 778, 781
- CTC Program (Computer and Telecommunication Coordinator), 187
- CTCs. *See* Community technology centers (CTCs)
- Cuba, 443
- Cultural diversity, 519
- Culture jamming, 307–309, 315
- Customs Service, 191
- Cyberbots/bots, 223–224, 285, 731
- Cyber Citizen Partnership, 188
- Cybercop units, defined, 199
- Cybercourt systems, 44–45

- Cybercrime:
 credit card theft/fraud, 29, 169, 182
 cyberfraud, 17–18
 defined, 172, 199
 overview/introduction, 41–43, 182–184
 types of, 183
 U.S. criminal justice system and (*see* Criminal justice system)
- Cyberlaw, 3–48
 censorship, 14–17
 clash of laws, 33–38 (*see also* Jurisdiction)
 “click” contracts, 18–19
 cybercrime, 41–43
 cyberfraud, 17–18
 defamation, 12–13
 defined, 45
 dispute resolution, 38–39
 e-commerce law, 18–23
 e-signatures, taxation, and spam, 19–21
 information security legal liabilities, 23–31
 insurance law, 31–33
 intellectual property, 5–12 (*see also* Intellectual property)
 copyright law, 5–7
 domain names and trademark law, 7–11
 patent, 11–12
 laws of linking, 39–41
 overview/introduction, 3–4, 43–45
 privacy concerns, 13–14
 terms defined, 45–48
 “terms of use” provisions, 21–22
 validity, 22–23
- Cyberlaw, global aspects, 627–660
 data protection, 660
 electronic signatures, 649–654, 660 (*see also* Electronic/digital signatures)
 encryption, 649–654, 660
 intellectual property, 654–659
 databases, 656–657
 ISP liability for third-party copyright infringement, 655–656
 software patents, 657–659
 international Safe Harbor principles, 660
 jurisdiction, 630–638
 overview/introduction, 627–629, 659–660
 privacy, 638–649, 660
 terms defined, 660
- Cybermetrics, 165
 CyberPatrol, 444, 450
 Cyberpirates, 8, 45–46
 Cybersettle, 12, 39
 CyberSLAPPs, 166
 Cybersmuggling Center, 191
- Cyberspace:
 defined, 172, 660
 term origin, 304
 warfare, 152
- Cybersquatting, 8, 45, 660
 Cyberstalking, 117, 122
 Cyberterrorism, 127–173
 acts, 129–131
 controlling, 155–170
 business and industry, 158–161
 general strategies, 156
 government, 161–167
 higher education institutions, 168–169
 information technology professionals, 156–158
 institutions, organizations, and conferences, 167–168
 small business and individuals, 169–170
- defining, 91, 135–144, 172
 communication in terrorism, 141
 definitions in use, 136–138
 extended definitions, 138–140
 five-level operational model, 141–144
 support for conventional terrorism, 140
- examples of, 129–131, 139
 how it occurs, 144–152
 convergence of physical and virtual worlds, 144–145
 vulnerabilities, 145–146
 overview/introduction, 127–128
 predictions about, 170–171
 risks, three categories, 131
 sponsors and support, 132–155
 statistics about, 143, 147, 163
 threats versus acts, 138
 tools of, 146–148
 warnings about, 131–135
 worldwide perspective, 154–155
- Dallas Regional Computer Forensic Lab, 397, 398, 400
Daniels v. Worldcom Corp., 800
Danish Newspaper Publishers Association v. Newsbooster.com, 41
 Darknet, 453
 DARPA, 843
 Databases, and intellectual property issues, 656–657
 Data encryption. *See* Encryption
 Data mining, 283, 285
 Data obfuscation, 360
 Data Processors International (DPI), 30
 Data protection, defined, 660
 Data quality, privacy issues of, 413
 Data recovery, 394, 401
 Data Recovery Agent (DRA), 366
 Data reduction, 395, 401
Daubert v. Merrell Dow Pharmaceuticals, Inc., 112, 377, 381
 DCC (Dental Content Committee), 555
 DDoS. *See* Distributed denial of service (DDoS)
 attacks
 DeCSS, 16, 444
 Deep linking, 39–40
 Defamation, 12–13, 46
 Defense(s), in criminal justice system, 105–110, 117–119
 affirmative, 105, 117–119
 choice of evils, 106
 defense of others, 106, 108
 defense of property, 106, 108
 duress, 106
 failure of proof, 105–106
 insanity, 106
 self-defense, 106
 Trojan horse defense, 118
 Defense attorneys, 102–103

- Defense-in-depth principle, 778
 Defense Satellite Communications System (DSCS), 734
 Defensive information operations, 748–749, 766–767
 de Guzman, Onel, 120–121
 Dell, 26
 Demilitarized zone (DMZ), 769
 Democracy, principles for electronic, 621
 Democratic deficit, 622
 Demographic groups and Internet/technology use, 515, 516, 517, 520, 521, 523
Dendrite International Inc. v. John Doe no. 3, 474–475
 Denial of service (DoS) attacks:
 cost to victims of, 26
 defined, 172, 781
 distributed denial of service (DDoS) attacks, 26, 29, 46, 148–150, 156, 170
 e-government concerns, 570
 preventing, 156
 wireless attacks, 753
 Dental Content Committee (DCC), 555
 Deontology, 74, 75, 91
 DES. *See* Digital Encryption Standard (DES)
 Deutsche Bank, 27
 DHS. *See* Homeland Security, Department of (DHS)
Diamond v. Diehr, 657
 Dick, Ronald, 140
 Digital, defined, 781
 Digital Divide, 513–531, 606–609, 622
 ability to create content, 519, 520
 access outside of homes, 517
 broadband access, 520–521, 530–531
 Community Technology Centers (CTCs), 531
 complex solutions, 527–530
 connectivity, 517
 defined:
 new definitions, 518–521
 original definition, 514–515
 simple, 622
 disabilities and, 519–520
 Federal Communications Commission (FCC), 531
 General Educational Development (GED), 531
 importance of closing, 526–527
 international, 522–526, 607, 669
 access, 524–525
 connectivity, 524
 deterrents to global e-governance, 606–609
 policy, 525
 quantitative national differences, 525
 UN Technology and Communications Index, 523–524
 literacy, 518
 overview/introduction, 513–514, 530
 “problem among many,” 517–518
 “problem solved,” 515–518
 recent data, 521–522
 relevance, 518–519
 S-curve pattern of diffusion, 516
 statistics/demographics, 515, 516, 517, 520, 521, 523
 Digital Encryption Standard (DES), 362, 365
 Digital Equipment Corporation (DEC), 249
 Digital evidence. *See* Evidence, digital
 Digital footprints, 689
 Digital identity. *See* Identity, digital
 Digital Millennium Copyright Act of 1998 (DMCA), 5–7, 46, 104, 185, 227–233, 239, 343–344, 444, 654–655, 656, 810
 Digital Pearl Harbor exercise, 132, 133–134, 140, 164
 Digital rights management (DRM), 602–603, 613, 714–716
 Digital signatures. *See* Electronic/digital signatures
 Digital tokens, 462, 463
 Digital world/virtual world/cyberspace, defined, 172
 Dilution of trademark, 8–9
 Direct exploitation of leakage channels, 699
 Direct/internal penetration attacks, 746
 Direct key attack, 768
 Direct mail, 255
 Direct Marketing Association (DMA), 261, 263, 264, 277
 Directory services, 504
 Disabled persons:
 definition, 825
 Digital Divide and, 519–520, 522
 employee e-mail/Internet use policies and, 801–802
 Disaster(s):
 potential computer and network disasters, 835
 preparing for, 847–849
 recovery, 850
 steps to take when disaster strikes, 849
 Disclaimer, defined, 825
 Disclosure, tort of, 411
 Discover card, 30
 Discrimination/harassment issues, 800–801, 814
 Dispute resolution, 9–11, 38–39, 44
 Disruption of availability, 727
 Distributed denial of service (DDoS) attacks, 26, 29, 46, 148–150, 156, 170. *See also* Denial of service (DoS) attacks
 DMCA. *See* Digital Millennium Copyright Act of 1998 (DMCA)
 DMZ (demilitarized zone), 769
 DNA testing, 483
 DNS (domain name system) hacking/poisoning, 148–150
 Document retention policies, 821
 Documents, identity, 496–498
Doe v. 2themart.com Inc., 471, 472, 473
Doe v. Ashcroft, 470
 Domain names:
 anonymous domain registrants, 473–477
 Anticybersquatting Consumer Protection Act of 1999 (ACPA), 8–9, 45
 cybersquatting, 8, 660
 defined, 91
 dispute resolution process, ICANN’s, 9–11
 legal weapon trade-offs, 11
 Uniform Domain-Name Dispute-Resolution Policy (UDRP), 9
 DNS (domain name system) poisoning, 148–150
 intellectual property and, 69–70
 market in buying/selling of, 8
 trademark law and, 7–11
 Do Not Call list, 482
 DoS. *See* Denial of service (DoS) attacks

- Double-blind bid (Cybersettle.com), 39
DoubleClick, Inc. Privacy Litigation, In re, 221
 Double jeopardy, 122
Douglas v. Hustler Magazine, 411
 Dow Jones, 36, 634
Dow Jones v. Gutnick, 36
 DRM. *See* Digital rights management (DRM)
 DSCS (Defense Satellite Communications System), 734
 Dual criminality, defined, 691
 Due process, 265–266, 409
 Duplicate digital evidence, 401
 Duress defense, 107
DVDCAA v. Bunner, 16–17
 Dyk, Anthony, 341
- Eagle Investment Systems, Corp. v. Tamm*, 219
 EAL-4, 579, 580
 Earthlink, 284
 eBay, 7, 26, 41, 213, 237, 494, 614
eBay, Inc. v. Bidder's Edge, Inc., 41, 213
 ECCM algorithms. *See* Electronic counter-countermeasures (ECCM)
 E-commerce law, overview, 18–23
 Economic Espionage Act of 1996 (EEA), 184, 185, 225–227, 239
 ECPA (Electronic Communications Privacy Act of 1986), 216, 416, 417, 418, 419, 432
 E-Data Corporation, 12
 Education. *See* Demographic groups and Internet/technology use
Edward Felten, et al. v. Recording Industry Association of America, Inc., et al., 228
EF Cultural Travel v. Zefer Corporation, 223–224
 Effects, jurisdiction based on, 35–36, 633–634
 EFS (Encrypted Files System), Microsoft, 365, 366
- E-government:
 definitions, 563–565
 general, 564
 U.S. government-specific, 564–565
 interactive processing, 566–567
 overview/introduction, 563, 586–587
 program types, examples, 565–567
 publishing, 565–566
 service delivery, 567
 terms defined, 587–588
 transaction processing, 567
- E-government, global, 591–622
 consistency and coordination of global information, 604–606
 defined, 622
 deterrents to, 606–609
 evolution of, 593–598
 current dimensions and limitations, 594–596
 localized accountabilities, 596
 problems of scale for information accuracy and security, 596–598
 technology and the state, 593–594
 global information commons, 600–603
 high-risk areas of global information, 615–620
 economic and financial, 615–616
 environmental, 617–618
 health, 618–619
 legal and administrative, 616–617
 transport, 619–620
 non-government actors and government information, 609–614
 citizens without borders, 613–614
 corporate sector, 609
 overview/introduction, 591–593, 620–622
 responsiveness, monitoring, and adaptation of global information, 603–604
 taxation and representation, 600
- E-Government Act of 2002, 564
- E-government security issues/measures, 567–578
 availability, 568–573
 classes of attacks (physical/logical), 572
 denial of service concerns, 570
 fault-related availability concerns, 568–569
 individual or informally organized hackers, 570–571
 intrinsic availability concerns, 569–570
 logical attacks, 572–573
 nonstate organizations, 571–572
 physical attacks, 572
 sources of denial of service attacks, 570
 state-sponsored attacks, 572
 availability, security mechanisms and techniques for, 578–579
 confidentiality and privacy, 576–578
 distinguishing confidentiality and privacy issues, 576–577
 impacts on operations, 577–578
 impacts or consequences of unauthorized exposure, 577
 legal issues, 578
 loss of confidence in institutions and service delivery mechanisms, 577
 vulnerabilities/threats, 577
 confidentiality and privacy, mechanisms/techniques for, 581–582
 cryptographic mechanisms, 582–583
 database design, 583
 protocol and operating system mechanisms, 582
 integrity, 573–576
 connection, 575
 data content, 573–574
 error-based integrity faults, 574
 intentional modification of data, 574–575
 nonrepudiation issues, 575–576
 integrity, mechanisms/techniques for, 579
 cryptographic mechanisms, 580–581
 protocol-based and operating system-based, 579–580
 security measures, implementation and management, 583–586
 certification and accreditation, 585–586
 interdependency of measures/mechanisms, 583
 policies, procedures, and infrastructures, 584–585
 program requirements, 584
- EHR (electronic health record). *See* Medical records
 EIRP (effective/equivalent isotropic radiated power), 734, 736, 781
Eldredge v. Ashcroft, 6
 Electrical blackouts, 129

- Electric grid, 129, 135
- Electromagnetic compatibility (EMC), 742, 781
- Electronic channels, information leakage and, 698, 703–706
- communications equipment, 704
 - credential sharing, 705–706
 - indirect inferential disclosure, 704
 - malware, 706
 - messaging systems, 703–704
 - phishing, 706
 - remote control, anonymizers, and tunneled protocols, 705
 - social networking and contact management sites, 704–705
 - Web, 704
 - Web publishing, blogs, and bulletin boards, 705
 - wireless networking, 705
- Electronic Civil Disobedience, 304
- Electronic Commerce Directive, 654
- Electronic Communications Privacy Act of 1986 (ECPA), 112, 237–238, 240, 804–806
- Electronic contract, 352. *See also* Contract(s)
- Electronic counter-countermeasures (ECCM), 743, 781
- Electronic/digital signatures:
- defined, 330–331, 353, 478, 587
 - digital signature algorithm (DSA), 581
 - digital signature standard (DSS), 581
 - encryption algorithms, 581, 582–583
 - encryption keys, private/public, 361, 463
 - methods of “signing” an electronic record, 331
 - overview/introduction, 19–21
 - public key cryptography, 331–332
 - requirements, online contracts, 329–330
 - technical overview, 651–652
- Electronic Disturbance Theater (EDT), 306
- Electronic footprint, 640
- Electronic Freedom Foundation, 469–476
- Electronic Frontier Foundation, 304
- Electronic Privacy Information Center, 648
- Electronic Signatures in Global and National Commerce Act of 2001 (E-SIGN), 19, 324–334, 348, 502, 653–654, 660
- consumer consent provisions, 328–329
 - defined, 660
 - UETA and, 327, 328, 330, 331, 332, 333, 334
- Electronics security (ELSEC), 749, 782
- Electronic trackers, 841
- Electronic transaction securities, 842–843
- Electronic warfare, 733, 782. *See also* Information warfare (IW); Wireless information warfare (WIW)
- Electronic workplace monitoring, 811–812, 825
- Eli Lilly and Company, 431
- ELSEC, 749, 782
- E-mail. *See* Employer e-mail/Internet use policies
- Emanations security (EMSEC), 749, 782
- Emergency response team, 843–844
- Emory University School of Medicine, defamation case, 12–13
- Employees:
- at-will, 814–816
 - constitutional restrictions, 807
 - contract law concerns, 798–799
 - disability and medical confidentiality issues, 801–802
 - discrimination and harassment issues, 800–801
 - federal labor law issues, 807–808
 - fiduciary duty, 211–213
 - Internet use by (*see* Employer e-mail/Internet use policies)
 - liabilities, security-related, 25–26
 - privacy of, 420–421, 803, 804–807
 - public sector, 817
 - rights, 798–808
 - union-represented, 816
- Employer e-mail/Internet use policies, 789–826
- anticipating new technologies, 797–798
 - blurring of workplace boundaries, 795–797
 - business use versus personal use, 794–795
 - communicating policy to employees, 822–823
 - complying with laws protecting employee rights, 798–808
 - constitutional restrictions, 807
 - contract law concerns, 798–799
 - disability and medical confidentiality issues, 801–802
 - discrimination and harassment issues, 800–801
 - Electronic Communications Privacy Act (ECPA), 804–806
 - federal labor law issues, 807–808
 - privacy tort concerns, 803
 - state workplace privacy statutes, 806–807
 - coordinating with other policies, 821–822
 - drafting, 792–794
 - employment status, special issues related to, 814–817
 - at-will employees, 814–816
 - public sector employees, 817
 - union-represented employees, 816
 - enforcing, 823
 - multinational employers, 817–821
 - overview/introduction, 789–791, 823–824
 - preventing criminal activity, 809–810
 - downloading copyrighted material without permission, 810
 - unlawful access to child pornography, 809–810
 - protecting trade secrets and other proprietary information, 808–809
 - purpose and function of, 791–794
 - reserving right to conduct electronic monitoring, 811–812
 - reserving right to discipline employees under the policy, 813–814
 - responding to government requests for electronic information, 812–813
 - scope of, 794–798
 - terms defined, 824–826
- EMSEC, 749, 782
- Encoding conversions, 506
- Encryption, 360–371, 842
- algorithms, symmetric/asymmetric (public key), 361
 - breaking (recovering passwords), 368–371
 - asking suspects, 368–369
 - automated tools, 369–370
 - breaking other accounts, 370–371
 - brute force attack, 370

- commercial and freeware tools, 371
- dictionary attacks, 369–370
- passwords on disk, 370
- rule-based attacks, 369
- social engineering, 368–369
- code, and censorship, 444
- defined, 91, 587, 660
- determining whether files are encrypted, 366
- Digital Encryption Standard (DES), 362, 365
- electronic signatures and, 649–654
- exportation regulation; United States law and international treaties, 650–651
- file system-level, 364–365
- individual files, 362–363
- keys:
 - defined, 463, 478
 - private key, 587
 - private key infrastructure (PKI), 650
 - public key algorithms/systems, 332, 361, 580, 587, 650–653, 773
 - public key infrastructures (PKI), 332, 580, 650–653, 773
- overview/introduction, 842
- programs, and public policy, 80–81
- regulatory models, 652–654
- what information can be encrypted, 362
- Windows encrypted file system, 365–366
- End point behavior control, 716–717
- End-point monitoring, 710
- End use license agreement (EULA), 341
- Engineering, reverse, 210, 229–231, 340–344
- Enterprise application integration, 504–508
- Enterprise/digital rights management (DRM), 602–603, 613, 714–716
- Enumeration (wireless attacks), 753
- Environmental information, 595, 617–618
- Environment discovery, leak detection, 715
- Equipment destruction, laws against, 117
- E-Rate program, 517
- Eritrea, 525
- Errors and omissions (E&O), 32
- Escalating privilege, 753
- E-SIGN. *See* Electronic Signatures in Global and National Commerce Act of 2000 (E-SIGN)
- ESPN, 10
- Ethics, 297–299, 315, 745
- Etoy campaign, 307
- EuroCAUCE, 279
- Europe/European Union, 38, 158, 185–186, 189, 193, 332, 612, 669, 682
 - computer security/legal protection, 82
 - Convention for the Protection of Human Rights, 442
 - Copyright Directive, 654, 656
 - criminal offence adopted, 154
 - cyber-crime convention, 195, 197
 - database, 41
 - Data Directive, 483, 484
 - Data Protection Act, 14
 - Electronic Commerce Directive, 636
 - Electronic Signature Directive, 330–331
 - employers, issues for, 817–818
 - Europol, 192–194, 683–684
 - Europol Drugs Unit (EDU), 193–194
 - free speech, 38, 55, 57, 86
 - hate speech, 61
 - jurisdiction, fundamental principles, 634–636
 - legal protection, 82
 - patents, 658, 659
 - pornography, 57
 - privacy, 74, 414–415, 421, 639, 643–644, 817–819, 825
 - spam, 262
- Evidence, digital, 357–402
 - challenges to law enforcement, 359–360
 - data obfuscation (encryption and steganography), 360
 - defined, 401
 - digital forensics and, 358–376
 - duplicate, 401
 - encryption, 360–371
 - forensic countermeasures, 384–392
 - file wiping, 385–386
 - trace evidence in RAM, 386–388
 - trace evidence in the swap and hibernation files, 388–389
 - trace evidence in unallocated space, 389–392
 - law enforcement: view of future of, 400–401
 - overview/introduction, 357–358
 - steganography, 371–376
 - terms defined, 401–402
 - validation of digital forensic tools, 377–384
 - volume/diversity of, 393–399
 - consequences for law enforcement, 394–395
 - explosion of diverse digital media, 398–399
 - solutions for data reduction, 395–397
 - using technology to cope, 397–398
- Evidentiary issues, criminal justice system, 112–113
- E-voting, 84–90
 - accuracy of technologies, 86–87
 - discriminatory effects on poor, 88–89
 - ethical arguments, for/against, 86–90
 - legal protection of voting, 85–86
 - moral legitimacy of, 86
 - security concerns, 89–90
 - turnout, effects on voter, 87–88
 - unreliability of existing technologies, 89
- Expedia, 494
- Experian, 255
- Exploitation, 728–729, 782
- Extensible markup language (XML), 491, 503, 506
- Extensible name service. *See* XNS (extensible name service)
- Extensible resource identifier. *See* XRI (extensible resource identifier)
- External open source intelligence, 708–709
- Extradition, 691
- Extreme detection with human inspection, 711
- Fair and Accurate Credit Transaction Act, 489
- Fair Credit Reporting Act (FCRA), 412
- Fair information principles, 413, 642
- Fair use, 4, 7, 22, 66
 - defined, 46, 353, 826
 - reverse engineering and, 229–230, 340–344
- False light, tort of, 411
- False negatives, 285
- False positives, 246, 285

- Falwell, Jerry, 10
 Family and medical leave, 801, 826
 Farey-Jones (*Theofel v. Farey-Jones*), 220–221
 Fault-tolerant systems, 834–835
 Federal Bureau of Investigation (FBI):
 Carnivore, 165, 166, 418, 470, 647, 648
 cases, number of, 394–395
 on digital evidence, 393
 “fbinformant,” 12–13
 hacking of sensitive information, 30
 Infraguard program, 670
 National Infrastructure Protection Center, 187
 PATRIOT Act, 167
 published list of top 20 security threats, 168
 spoofing, 255
 technology and, 398
 Federal Communications Commission (FCC), 531
 Federal Depository Library Program, 526
Federal Express Corp. v. Dutschmann, 799
 Federal Family and Medical Leave Act of 1993, 801
 Federal Information Security Management Act of 2002 (FISMA), 161, 584
 Federalist Papers, 465
 Federal Trade Act, 431
 Federal Trade Commission (FTC):
 cyberfraud, 17–18
 privacy, 427, 429–431
 spam, 247, 252, 255, 259, 261, 262, 265, 269, 271, 272, 275, 278
 Federal Trademark Dilution Act (FTDA), 8–9
 Federation (feature), 495, 510
Feist Publications v. Rural Telephone Service Co., 343, 657
 Felsenstein, Lee, 300
 Felten, Edward, 228
 Ferber Court, 116
Ferguson v. Friendfinders, 267
 Fiduciary duty, 211–213, 240
 Fifth Amendment. *See* Constitution of United States
 File descriptor attacks, 755
 File transfer protocol (FTP), 70, 91, 758
 File wiping, 385–386
 Filters/filtering devices, 62–63, 91
 Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act), 13, 412, 432, 483
 Firewalls, 146, 445–446, 487, 582, 765–766, 838
 defined, 453, 782, 839–840
 First Amendment rights. *See* Constitution of United States
 First effects, 730
 First-party cookie, 425
 FISA (Foreign Intelligence Surveillance Act of 1978), 416, 417–419, 432
Fischer v. Mt. Olive Lutheran Church, 806
 Flooding attacks, 573
 Flood Net, 306, 307
 Floppy disks, epitaph for, 398
 Florida, presidential election (2002), 86
 Florida’s Security of Communications Act, 806
 Flowers.com, 255
 Food and Drug Administration (FDA), 44
 Footprinting (wireless attacks), 753
 Footprints, digital, 689
Ford Motor Co. v. Lane, 16
 Foreign Intelligence Surveillance Act of 1978 (FISA), 416, 417–419, 432
 Foreign workplace laws, 819–821
 Forensic countermeasures, 384–392
 file wiping, 385–386
 trace evidence in RAM, 386–388
 trace evidence in the swap and hibernation files, 388–389
 trace evidence in unallocated space, 389–392
 Forensic evidence. *See* Evidence, digital
 Forensic image, defined, 401
Forest v. Verizon Communications Inc., 338
 Forward line of own troops (FLOT), 782
 Fractal patterns, 597, 620, 622
 Frame capture, 768
 Framework for Global Electronic Commerce, 628
 Framing, 39–40
Frampton v. Central Indiana Gas Co., 814
 France:
 French language, 38
 G8, 681
 Nazi memorabilia decision (*Yahoo! v. La Ligue Contre Le Racisme et L’Antisemitisme*), 37, 42–631, 636–368
 penal code, 185–186
 Franklin, Ben, 465
Fraser v. National Mut. Ins. Co., 221
 Fraud, 17–18. *See also* Cybercrime
 Freedom of Information Act, 648
 Freedom, 308
 Free software, defined, 315
 Free Software Foundation, 310
 Free speech, 54–65
 filtering devices, 62–63
 First Amendment, 16, 55, 73, 409, 410, 448, 466, 471, 473, 476, 477
 hate speech online, 60–64
 Internet issues, 56–65
 legal protection of, 55
 moral legitimacy of right to, 55–56
 search engines, 63–65
 spam, 61–62
 utilitarian justifications, 55–56
 web pornography and children, 56–59
 Fringe activity, Internet, 142
 FTDA. *See* Federal Trademark Dilution Act (FTDA)
 FTP (file transfer protocol), 70, 91
 Full Faith and Credit Clause of United States Constitution, 637
 Functional literacy, 518
 Fundamentalist Web sites, 612
 G8, 119–120, 122, 190, 681–682, 687
 Gallagher, Frank, 139
 Game theory, 135, 137
Garner v. Loomis Armored, Inc., 814
Garry v. John Hancock Mutual Life Insurance Co., 235, 803
 Gatekeeper argument, 477
 Gates, Bill, 245, 283–284, 285. *See also* Microsoft
 Gender. *See* Demographic groups and Internet/technology use
 General Agreement on Information Privacy (GAIP), 649

- General Agreement on Tariffs and Trade, 655
 General Educational Development (GED), 531
 General Motors, 820
 GeoCities, Yahoo!, 430
Geoff v. AOL, Inc., 19
 Geographic proximity, 596
 Germany, 55, 60–61, 186, 191, 442, 681
 GIF, clear, 425
Ginsberg v. U.S., 442
 GLB/GLBA. *See* Gramm-Leach-Bliley Act (GLBA)
 Global community services, 498, 510
 Global information commons, defined, 622
 Global information infrastructure (GII), 445
 Global issues:
 building global legal order, 188–190
 e-governance (*see* E-government, global)
 foreign workplace laws, 819–821
 globalization, 622
 high-risk areas of global information, 615–620
 economic and financial, 615–616
 environmental, 617–618
 health, 618–619
 legal and administrative, 616–617
 transport, 619–620
 international Digital Divide, 522–526
 international Safe Harbor principles, 660
 law enforcement (*see* Law enforcement, global)
 privacy laws, 413–415
 transnational policing and cybercrime, 190–194,
 199, 672–676
 Global Reporting Initiative (GRI), 610–611
 Global system for mobile (GSM) communications,
 782
Global Telemedia International Inc. v. Doe I, 472
 Global warming, 608
 GNU Privacy Guard, 362, 366, 367, 368
 Gnutella, 439
 Gohel, M. J., 153
 Goldman Sachs, 27
 Goods versus license, computer information products
 as, 344–347
 Goodyear, 8
 Google, 63, 451, 490
 Gordon, Thomas, 465
 Gore, Al, 514
 Government. *See also* E-government
 censorship, 447–450
 compulsory and voluntary cooperation between
 business and, 237–238
 cyberterrorism and, 161–167
 coordination, 162–164
 introspection and protection, 161–162
 legal and privacy concerns, 166–167
 surveillance and investigation, 164–165
 employers's responding to requests for electronic
 information, 812–813
 records, privacy issues, 412
 wiretapping/spying, 236–238, 410 (*see also* USA
 PATRIOT Act (Uniting and Strengthening
 America by Providing Appropriate Tools
 Required to Intercept and Obstruct
 Terrorism))
 Government Paperwork Elimination Act (GPEA),
 564
 GPG (GNU Privacy Guard), 362, 366, 367, 368
 GPS positioning devices, 725
Graham v. Oppenheimer, 13
 Gramm-Leach-Bliley Act (GLBA), 13, 412, 432, 483
Granhold v. Heald, 43
 Graphical user interface (GUI), 172
 Graphics or art department, and security task force,
 832
 Greece, 186
Greenberg v. National Geographic Society, 6
 Greenpeace, 611
 Grid infrastructure, aging, 129, 135
Griggs-Ryan v. Smith in footnote, 217
Griswold v. Connecticut, 73, 234
 Grokster, 6
 Group of Eight (G8), 119–120, 122, 190, 681–682,
 687
Grynberg v. Agri Tech, 24
 Guess! Jeans, Inc., 431
Gus' Catering, Inc. v. Microsoft Systems, 29
 Gutnick, Joseph, 36, 634
 Hack back defense, 110–111
 Hacker(s)/hacking:
 cracking versus, 84
 cyberterrorism and, 153
 defined, 91, 122, 172, 315
 generations/categories, 298–299
 game hackers, 298
 hackers/crackers, 298
 hacktivists, 299
 hardware hackers, 298
 microserfs, 296, 299, 300–304, 315
 open source/free software hackers, 299
 true hackers, 298
 hijacked computers, 256, 285
 “homeless hacker,” 103
 overview/introduction, 26–27
 simple versus aggravated, 116
 spamming and, 248
 success of, 17, 134–135
 tools, 146–147
 Hacker ethic, defined, 315
 Hacktivism, 295–316
 “all that is solid melts into the air,” 313–314
 antiglobalization/anticapitalism movements, 315
 categories of Internet usage and, 142
 culture jamming, 307–309, 315
 defined, 84, 91, 315
 Etoy campaign, 307
 examples, 307–309
 founding ethics, 297–299, 315
 free software, 309–313, 315
 microserfdom, 300–304, 315
 open source movement, 309–313, 316
 overview/introduction, 295–296, 314–315
 precision targeted satire, 309
 RTMark, 309
 source code, 316
 tactical media, 304–307
 terms defined, 315–316
 virtual sit-in, 304–307, 316
 Yes Men, The, 309
 Hague Conference on Private International Law, 38

- Halifax Summit, 681
 Hamidi, Kourosh, 269
 Handover, defined, 782
Hanson v. Denckla, 632
 Hardware, defined, 172
 Hardware/software groups, on security task force, 832
 Harmful forms of speech, 441–443
 Harassment issues, 800–801, 814
 Harvard.net, 8
 Hashes, 374–375, 395, 396, 402, 581, 771
 Hate speech, 60–64, 453
 Haves/have-nots, 514. *See also* Digital Divide
 Hawaiian Airlines (*Konop v. Hawaiian Airlines, Inc.*), 217, 218, 219, 804
 Hawke, Davis Wolfgang, 268
 Health and Human Services (HHS), 536, 556, 558
 Health information:
 privacy and (*see* Medical records)
 vulnerability of, 618–619
 Health Insurance Portability and Accountability Act (HIPAA):
 defined, 432, 782
 opt-in/out-out, 14
 privacy legislation, 14, 74
 privacy of medical records, 74
 provisions, 536, 538, 539, 541, 543, 545, 546, 547, 555, 751, 802
 standardization of data formats, 483
 Health insurance records, 412
 Health Level Seven (HL7), 541, 555
Heckel, 267
 Hegelian view, 67
 Hennessy, John, 169
 Hep-C Alert, 557
 HEW, 411–412
 Hewlett-Packard, 491
 Hibernation files, 388–389
 Higher education institutions, and cyberterrorism, 168–169
Hibel v. Sixth Judicial Circuit Court of Nevada, 468
 Hijacked computers, 256, 285
Hill v. Gateway 2000, Inc., 338
 HinduUnity.org, 449
 HIPAA. *See* Health Insurance Portability and Accountability Act (HIPAA)
 HLB Technology, 343
 Hoffman, Abbie, 301
 "Hole in the wall" experiment, New Delhi, 528
 Holistic approach, 160
 Holmes, Oliver Wendell, 476
 Homebrew Computer Club, 300
 Homeland Security, Department of (DHS), 132, 164, 167, 172, 198, 484
 Homeland Security Act (2002), 30
 Homeless hacker, 103
Homo economicus, 302
 Honduras, 191
 Hospital as example of wireless information warfare
 in practice:
 attack, 756–763
 defense, 763–777
 vulnerabilities, 749–756
 Host-based intrusion detection system (h-IDS), 763–765
 Host identity, 503, 510
 Hostile work environment, 826
 Hosting service, 503
 Hotmail, 222, 494
 Human behavior detection, 713
 Human channels, leakage of information and, 698, 706–708
 misdirection of communications, 707
 personal relationships, 707
 social engineering, 707
 use of communications technology in public places, 706–707
 use of public facilities, 707–708
 word of mouth, 706
 Human inspection, extreme detection with, 711
 Human Rights Watch, 611
 Hunter, Richard (*World without Secrets*), 167
 Hussein, Saddam, 151, 152
 Hustler (*Douglass v. Hustler Magazine*), 411
 Hypertext transfer protocol (HTTP), 497
 Hypertextual (term's first appearance), 300
 "I accept" button, 331, 334, 338
 I-ACERT security certification program, 158
 IBM, 301, 491, 509
 Identification badges, 841
 Identity, digital, 481–511
 consumers and, 494–495
 data sharing permissions and contracts, 500–502
 defined, 481–482, 510
 enterprise application integration and, 504–508
 future of, 509–510
 illustrated, 492–494
 overview/introduction, 481
 players, 508–509
 privacy and, 482–485
 services, 502–504
 Web services and, 490–491
 Identity documents, 496–498, 510
 Identity ID, defined, 497, 510
 Identity linking, 498–500, 510
 Identity name, defined, 511
 Identity server, 496, 511
 Identity service provider, 496, 511
 Identity theft, 485–490
 commonsense things to protect yourself, 487–488
 Identity Web, 495–496, 511
 IIHI (Individually Identifiable Health Information), 538, 558
I Lan Systems v. Netscout Service Level Corp., 24, 338
 Illich, Ivan (*Tools for Conviviality*), 300
 "I Love You" virus, 26, 170, 837
 IMAP (Internet message access protocol), 771, 772
 Incident response, 775–776
 Indemnity provisions, 22
 India, 188, 528, 639, 651
 Indirect exploitation of leakage channels, 699
 Indirect/external sensor attacks, 746
 Indirect inferential disclosure, information leakage and, 704

- Individual(s):
 - competing interests, business versus, 233–234
 - corporate spying and, 233–236
 - cyberterrorism and, 169–170
 - international privacy law, and individual participation, 414
- Indonesia, 191
- Information, four types needed by governments/citizens, 595
- Information aggression, domains of, 726, 727, 728
- Information-based warfare (IBW)/Information operations (IO), defined, 782
- Information corruption, 733
- Information leakage, 695–720
 - correction, 718–719
 - detection, 708–713
 - account misuse detection, 712
 - behavioral methods, 711
 - data driven, 711
 - end-point monitoring, 710
 - environment discovery, 713
 - external open source intelligence, 708–709
 - extreme detection with human inspection, 711
 - human behavior detection, 713
 - ingress/egress monitoring, 709–710
 - internal intelligence detection, 709
 - messaging and communications analysis, 709
 - network and system anomaly detection, 713
 - physical inspection, 713
 - policy- or lexicon-derived methods, 711
 - retention monitoring, 710
 - statistical methods, 711
 - web log analysis, 712
 - direct/indirect exploitation of channels, 699
 - electronic channels, 698, 703–706
 - communications equipment, 704
 - credential sharing, 705–706
 - indirect inferential disclosure, 704
 - malware, 706
 - messaging systems, 703–704
 - phishing, 706
 - remote control, anonymizers, and tunneled protocols, 705
 - social networking and contact management sites, 704–705
 - Web, 704
 - Web publishing, blogs, and bulletin boards, 705
 - wireless networking, 705
 - human channels, 698, 706–708
 - misdirection of communications, 707
 - personal relationships, 707
 - social engineering, 707
 - use of communications technology in public places, 706–707
 - use of public facilities, 707–708
 - word of mouth, 706
 - overview/introduction, 695–697, 698–699, 719–720
 - physical channels, 698, 699–703
 - cell phones, cameras, music players, and PDAs, 701–702
 - classic spy equipment, 702
 - disposal of media and equipment, 702–703
 - emanations, 702
 - laptops and corporate PDAs, 703
 - media, 700–701
 - office equipment, 700
 - voice and video communications, 701
 - protection and prevention, 714–718
 - authentication and authorization, 716
 - clean rooms, 714
 - end point behavior control, 716–717
 - enterprise/digital rights management (DRM), 714–716
 - Internet and communications access blocking, 717
 - keeping clear of bad people, 718
 - pervasive surveillance, education, and training, 718
 - portable secure environments, 717–718
 - scope of illegitimate use of legitimate authority in the context of leakage, 697–698
- Information literacy, 518
- Information privacy, 73–81
 - corporate use of personal information, 77–78
 - encryption programs and public policy, 80–81
 - Internet issues, 77–81
 - legal protection of, 73–74
 - moral legitimacy of rights of, 74–75
 - public and private information, 75–76
 - state databases, 79–80
- Information security (INFOSEC), 749, 782
- Information security legal liabilities, 23–31
 - computer software and hardware manufacturers, 24–25
 - employee security-related liabilities, 25–26
 - hackers, crackers, and viruses, 26–27
 - victims, 28–31
- Information Sharing and Analysis Center (ISAC), 158, 172–173
- Information Technology Management Reform Act of 1996, 584
- Information technology professionals, cyberterrorism and, 156–158
- Information warfare (IW), 783. *See also* Electronic warfare; Wireless information warfare (WIW)
- Infraguard program, FBI's, 670
- Infrastructure, 129, 135, 187, 584–585
- Ingress/egress monitoring, 709–710
- In re Alappat*, 658
- In re Boureguad*, 658
- In re DoubleClick, Inc. Privacy Litigation*, 221
- In re Intuit Privacy Litigation* footnote, 222
- In re Pharmtrak, Inc.*, 218, 805
- In re Toys R Us, Inc. Privacy Litigation*, 221
- Instant messaging, 797
- Institutions/organizations/conferences, cyberterrorism and, 167–168
- Insurance law, 27, 31–33
- Integrated Capital Associates (ICA), 220
- Integrity:
 - accuracy and, 834
 - connection, 575
 - corruption of, 728
 - cryptographic mechanisms, 580–581
 - data content, 573–574
 - defined, 587
 - e-government and, 573–576

- Integrity (*Continued*)
 error-based integrity faults, 574
 intentional modification of data, 574–575
 nonrepudiation issues, 575–576
 protocol-based and operating system-based mechanisms, 579–580
 wireless information warfare and, 727–732
- Intel, 118
- Intel v. Hamidi*, 214, 269, 446
- Intellectual property:
 copyright law, 5–7, 66, 655–656
 crime involving, 99, 122
 databases, 656–657
 defined, 46, 91, 122
 global cyberlaw, 654–659
 Internet issues, 69–72
 domain names, 69–70
 illicit copying, 70–71
 plagiarism, 71–72
 ISP liability for third-party infringement, 655–656
 legal protection of, 65–66
 moral legitimacy of rights of, 66–69
 Hegelian view, 67
 Lockean view, 66
 utilitarian argument, 67–68
 overview/introduction, 5–12
 patent law, 65
 software, 657–659
 trademark law, 65
 Web sites resources, 65
- Intentional threats:
 defined, 850
 identification of, 836–838
 table of popular ones, 837
- Interactive processing, 566–567, 587
- Intercept, defined, 217
- Internal/external threats and vulnerability, 836
- Internal intelligence detection, 709
- Internal Revenue Service (IRS), 398, 526
- International issues. *See* Global issues
- International Security, Trust, and Privacy Alliance (ISTPA), 501
- International Shoe Company v. Washington State*, 34
- Internet:
 communications access blocking and, 717
 defined, 353
 terrorism, and categories of usage, 142
- Internet control message protocol (ICMP), 573
- Internet Corporation for Assigned Names and Numbers (ICANN), 9–11, 16, 38, 46, 336, 601, 629
- Internet Engineering Task Force (IETF), 601
- Internet Explorer, 422
- Internet Fraud Complaint Center, 689
- Internet message access protocol (IMAC), 783
- InternetNeutral, 39
- Internet Protocol (IP) address, 144, 158, 173, 423–424, 432, 446
- Internet service providers (ISPs):
 censorship and, 451
 liability for third-party copyright infringement, 655–656
- Internet Tax Freedom Act (1998), 19–20
- Interoperability, 230
 with legacy systems, 742–743
- Interpol (International Criminal Police Organization), 119–120, 122, 192–194, 393, 684, 685–686
- Introduction service, 504
- Intrusion, tort of, 411
- Intrusion detection system (IDS), 762, 763, 769, 778, 783, 838–840
- Intuit Privacy Litigation, In re* footnote, 222
- Investment fraud, 17–18
- Iran, 153
- Iraq, 152, 153
- Israel, 651
- I-Sys Inc. v. Softwares Inc.*, 335
- Italy, 191, 681
- ITU (International Telecommunications Union), 610
- Jamming, culture, 307–309, 315
- Jamming of communications, 741
- Japan, 38, 158, 186, 190, 465, 673, 681
- Jefferson, Thomas, 465
- Jeopardy, double, 104–105
- Joe job, 487
- John Doe complaints, 7, 12
- John Doe spammer, 265
- Johnson, David, 475
- John the Ripper, 371
- Joint application design (JAD), 833
- Joint Chiefs of Staff (JCS), 725
- Joint Commission on Accreditation of Healthcare Organizations (JCAHO), 556
- Jones, Shirley (*Calder v. Jones*), 35, 632, 633
- JPhide, 376
- Jurisdiction:
 clash of laws, 33–38
 CoE's Cybercrime Convention on, 679
 defined, 47
 effects test, 35–36, 633–634
 global aspects of cyberlaw, 194–196, 630–638
 classic U.S. jurisdiction principles, 632–633
 difficulties of harmonizing approaches, 194–196
 enforcement jurisdiction and the Yahoo! case, 636–638
 fundamental jurisdictional principles under international law, 630–632
 fundamental principles of jurisdiction under European law, 634–636
 overview, 630
 to prescribe, 631
- Jury trial, 104, 122
- Justice department, 30, 187, 188, 258, 463
- Justice system. *See* Criminal justice system
- Justification defense (self-defense), 107
- Kansas, voting problem in, 89
- Kassebaum-Kennedy Bill. *See* Health Insurance Portability and Accountability Act (HIPAA)
- KaZaA, 232, 439
- Kelleher v. City of Reading*, 817
- Kennan, George, 466
- Kennedy-Kassebaum Bill. *See* Health Insurance Portability and Accountability Act (HIPAA)
- Kentucky Fried Computers*, 301

- Kerchoffs' principle, 748
 Kernel flaws, 755
 Kerr, Orrin, 166–167
Keavance Oil Co. v. Bicon Corp., 210, 342
 Key IDs, 767
 King, Martin Luther, Jr., 256
Konop v. Hawaiian Airlines, Inc., 217, 218, 219, 804
 Korea, 280
 Kraft Foods, 253
 Kushner, Harvey, 154
 KVM (shared keyboard, video, mouse), 135
 Kyoto Agreement, 604
- L0phtCrack, 371
 Labor laws, federal, 807–808
 Labovitz, Craig, 149
 Lamo, Adrian, 103
 Larkin, Dan, 255
 Law. *See* Cyberlaw; Cyberlaw, global aspects
 Law enforcement, cybercrime and, 181–199, 667–691
 - balancing order and liberty, 194–197
 - balancing privacy and, 416–419
 - building global legal order to protect computer security, 188–190
 - burden shifting approach, 196
 - Convention on Cyber-Crime, defined, 199
 - coordination of law and law enforcement, 194–196
 - cybercop units, 199
 - cybercrimes, 199
 - definitions, 199
 - digital evidence (*see* Evidence, digital)
 - establishing computer security through national laws, 184–186
 - information arms race, 485
 - legal systems, 199
 - national laws concerning computer security, 186–188
 - overview, 41–43, 181–184, 197–199
 - recruitment/training of computer specialists, 196
 - spam, interest in, 255
 - technology, policing, 196–197
- Law enforcement, global, 667–691
 - cooperation, global/regional, 680–690
 - APEC, 686–688
 - ASEAN, 682–683
 - European Union and Europol, 683–684
 - G8 Senior Experts Group on Transnational organized crime, 681–682
 - Interpol (International Criminal Police Organization), 685–686
 - OECD, 684–685
 - Council of Europe Cybercrime Convention, 676–680
 - computer-related offenses, 677–678
 - content-related offenses, 678–679
 - copyright infringement, 679
 - jurisdiction, 679
 - procedural powers, 679–680
 - criminality and computer crime, 670–672
 - international policing, 190–194, 672–676
 - cross-border law enforcement, 199
 - role of Interpol and Europol, 192–194
 - variations, 191–192
 - overview/introduction, 667–670
 - United Nations convention against transnational organized crime, 674–675
- Law merchant, 353
Lawrence v. Texas, 235
 Leaks. *See* Information leakage
 Least privilege concept, 546
 Lederle Labs, 327
 Legacy systems, 742–743
 Legal and administrative information, vulnerability of, 616–617
 Legal department, and security task force, 832
 Legal protection:
 - free speech, 55
 - information privacy, 73–74
 - intellectual property, 65–66
 - voting, 85–86
- Legal systems, defined, 199
 Legal weapon trade-offs, 11
 Lessig, Laurence, 248, 282, 283, 443–444, 448
 Letter rogatory process, 120
 Levine, Noah, 476
Lex mercatoria, 321
 Liabilities, legal:
 - commercial general liability (CGL) insurance policies, 31–33
 - computer software/hardware manufacturer, 24–25
 - disclaimers of, 21–22
 - employees, 25–26
 - information security, 23–31
 - Internet service providers, third-party copyright infringement, 655–656
- Liberty, balance of order and, 194–197
 Liberty Alliance, 494, 495, 496, 502, 503, 508, 511
 Liberty Principle, 56
 Library of Congress, 393
 Libya, 153
 License, defined, 353
 Line-sight radios, 783
 Linking:
 - bypassing home pages, 40
 - identity, 498–500, 510
 - laws of, 39–41
- Linux, 67, 311, 385, 388, 391–392, 659, 752
 List treaty, 691
 Literacy, types of, 518
 Local access portion, 497
 Localized accountabilities, e-government, 596
 Lockean view, 66
 Logical attacks, 572–573
 Long-arm statutes, 47
 Lorenz attractor, 597, 598
 Los Alamos Lab, New Mexico, 544
 Louisiana License Act, 342
 Love Bug virus/worm, 120, 121, 183
 LowSan virus, 27
 Low probability of detection (LPD), 741, 783
Lucker Manufacturing v. Home Insurance Co., 32
 Lyon Group, 682, 683
- Maastricht, Treaty of (1992), 193, 683
 MAC. *See* Media access control (MAC)
 Madison, James, 465
 Mafiaboy, 26, 27

- Magic Lantern, FBI's, 166, 418
 Mail transfer agent (MTA), 770–771, 783
 Malicious code introduction, defense against, 770–772
 Malicious Crypto Virology, 770
 Malware. *See* Viruses/worms/malware
M. A. Mortenson Co., Inc. v. Timberline Software Corp., 24, 25, 338, 346
Maquiladoras, 314
 Maran, Murasoli, 530
 Marino, Dan, 10
Market Development Corp. v. Falme-Glo Ltd., 326
 Marxism, 313, 314–315
 Massachusetts drivers license renewal, 526
 Massachusetts Water Resource Authority (MWRA), 159–160
 MasterCard, 29, 30
 McCain, John, 275
 McDonald's, 8
 McIntyre, Margaret, 466–467
McIntyre v. Ohio Elections Commission, 466–469, 475, 476, 477
McLaren v. Microsoft Corporation, 799, 803
 MD5 hash, 374, 396, 402, 771
 Media access control (MAC), 397, 751, 758, 767, 769, 783
 Mediations, 39
 Medical Privacy Coalition, 557
 Medical records, 535–558
 ANSI X12N, 541–542, 555, 558
 covered entities (CEs), 557
 diversity of health data, 536
 electronic health record (EHR), 537, 557
 pros/cons, 539
 structure and functions, 538–539
 electronic health record (EHR) security concerns, 543–546
 access, 543–544
 external threats, 544–546
 identifying threats, 544
 internal threats, 545
 electronic health record (EHR) security solutions, 546–554
 patients, 554
 service providers, 553–554
 step-by-step, 547–553
 virtual policy notebook, 547
 employee policies, and confidentiality, 801–802
 grassroots privacy groups, 556–557
 Health Level Seven (HL7), 542–543, 558
 Individually Identifiable Health Information (IIHI), 558
 oversight bodies, 555–556
 overview/introduction, 535–537
 paper record, pros/cons, 537–538
 paradox of health data, 536–537
 patient advocacy groups, 557
 patient health record, 558
 portable health record (PHR), 537, 540–541, 558
 privacy and, 412
 regulations, policies, and organizations, 554–557
 standards bodies, 541–543
 standards organizations, 541–543, 555
 terms defined, 557–558
 threats, 558
 U.S. national regulations, 554–555, 558 (*see also* Health Insurance Portability and Accountability Act (HIPAA))
 value of health data in an information society, 537
 Merten, Stefan, 312
 Messaging and communications analysis, 709–711
 behavioral methods, 711
 data driven, 711
 end-point monitoring, 710
 extreme detection with human inspection, 711
 ingress/egress monitoring, 709–710
 policy- or lexicon-derived methods, 711
 retention monitoring, 710
 statistical methods, 711
 Messaging systems, information leakage and, 703–704
 Metadata, 402
 Metadirectory products, 509
 Mexico, 185, 673
MGM Studios v. Grokster, 6
 Miami Electronic Crimes Task Force, 98
Miami Herald Publishing Co. v. Tornillo, 467
 Michigan, cybercourt in, 44
 Micro CDs, 540
 Microserfs, 296, 299, 300–304, 315
 Microsoft:
 anonymity and, 12
 Balmer on “free software,” 310–311
 Carp v. Microsoft Network, 338
 community groups and Digital Divide, 529
 Crispi v. The Microsoft Network, 19
 EFS (Encrypted Files System), 365, 366
 on free software, 311
 headquarters’ atmosphere, 302
 McLaren v. Microsoft Corporation, 803
 “mindshare,” 312
 Network, 494
 Palladium, 508
 Passport, 494, 495, 508, 511
 patches, 157
 patent applications for Internet applications, 12
 recognition of need for improving security, 690
 SmartScreen, 254
 spam:
 Anti-Spam Coalition, 270
 filtering spam for Gates, 245
 John Doe lawsuits, 265
 spoofing, 255
 Trustworthy Computing initiative, 508
 Windows, Messenger Service, 270
 Windows 9x (no longer supporting), 254
 Word, temp files, and trace evidence, 390–391
 X-Box, 308
 Middle East, 612
 Military:
 revolution in military affairs (RMA), 151
 system requirements unique to, 741–742
 Mill, John Stuart, 55–56
Miller v. California, 440
 MIMESweeper, 451
 Mindshare, 312
 Minimalist legislative approach, 652
Miranda, 96

- Mirror disks, 835
 Mitnick, Kevin, 100, 145
 Mixmaster, 464
 Mobility:
 classifications, 735–736
 defined, 783
 Mobile IP, 733
 Moldavia, 11
 Monitoring, workplace, 811–812, 825
 Moral legitimacy:
 of e-voting, 86
 of free speech rights, 55–56
 of information privacy rights, 74–75
 of intellectual property rights, 66–72
 Morgan Stanley, 27
 Morpheus, 232
Mortenson Co., Inc. v. Timberline Software Corp., 24,
 25, 338, 346
Moseley v. Secret Catalogue, 9
 Motion Picture Industry Association of America, 231
Moulton v. VC3, 282
 Mozena, John, 252
 MP3 files, 70, 91
 MTA. *See* Mail transfer agent (MTA)
 Mueller, Robert, 165
Muick v. Glenayre Electronics, 236
 Multinational employers, special issues for, 817–821
 Muris, Timothy, 260, 271
 Music files, sharing, 439
 Mutual legal assistance (MLA), 120, 121, 673, 676,
 680, 683, 684, 691
 Mutual legal assistance treaties (MLATs), 120, 691
 MyDoom worm, 670
- N2H2 Internet Filtering, 450
 NAACP, 466
 Napster, 4, 6, 7, 70–71
National Bellas Hess v. State of Illinois, 20
 National Coalition for Patient Rights, 557
 National Council of Commissioners on Uniform
 State Laws (NCCUSL), 324
 National Cybercrime Training Partnership (NCTP),
 188
 National Cyber Security Alliance (NCSA), 156
National Enquirer case, 633
 National Geographic Society, 6
 National Institute for Standards and Technology
 (NIST) Computer Forensics Tool Testing
 (CFTT), 378
 National Labor Relations Act of 1935 (NLRA), 804,
 807–808
 National Labor Relations Board (NLRB), 816
 National Science Foundation (NSF) grants, 169
 National Security Letter (NSL), 470
 National Stolen Property Act, 184
 National Telecommunications and Information
 Administration (NTIA), 514, 515, 517, 519,
 522, 526
 A Nation Online, 515, 517
 Falling through the Net, 514, 515
 National White Collar Crime Center (NW3C), 188
 Nazi memorabilia decision (*Yahoo! v. La Ligue Contre
 Le Racisme et L'Antisemitisme*), 37, 42–631,
 636–668
- NCPDP (National Council for Prescription Drug
 Programs), 555
 Negotiation, defined, 511
 Nelson, Ted (*Computer Lib/Dream Machines*), 300
 NET Act. *See* No Electronic Theft Act of 1997
 (NET)
 Netegrity, 509
 Netiquette, 47
 Netscape, 422
Network (movie), 245
 Network architecture classifications, 734–735
 Network attached storage devices (NAS), 397
 Network load balancing, clustering and, 775
 Network and system anomaly detection, 713
 NetZero, 464
 New Delhi, 528
 Newsbooster.com, 41
 Newsletters, e-mail, 260
 New York, 330
New York Times:
 employees fired for trading dirty jokes email
 system, 420
 hacking incidents, 83, 103
 New York Times v. Tasini, 6
New York v. Ferber, 116
 New Zealand, 639, 820
 Nichols, Terry, 105
 Nigerian scams, 461
 9/11:
 defined, 172
 era following, 33, 129, 131, 154–155, 165, 170,
 198–199, 482
 Nintendo, 229
 NIST (National Institute of Standards), 555
 No Electronic Theft Act of 1997 (NET), 6, 47, 184,
 185
 Non-government actors and government
 information, 609–614
 citizens without borders, 613–614
 corporate sector, 609
 Nonrepudiation:
 defined, 587
 e-government issues, 575–576
 of origin, 843
 of receipt, 843
 North Dakota Medical Association, 557
 Norvag worm, 670
 Notice:
 and consent requirements, online contracts, 328
 privacy and, 411
 Novell, 509
 NTIA. *See* National Telecommunications and
 Information Administration (NTIA)
 NUBC (National Uniform Billing Committee), 555
 NUCC (National Uniform Claims Committee), 555
 Nuremberg Files case, 15, 60
- OAS. *See* Organization of American States (OAS)
 OASIS (Organization for the Advancement of
 Structured Information Standards), 496, 508
 Oblix, 509
 Obscenity, 440
 Occupational literacy, 518
O'Connor v. Ortega, 817

- Oddworldz.com, 80
- OECD. *See* Organization for Economic Cooperation and Development (OECD)
- Office of management and Budget (OMB), 564, 584
- Office of Technology Assessment (OTA), 576
- Ohio, 266
- McIntyre v. Ohio Elections Commission*, 466–469, 475, 476, 477
- Ohralik v. Ohio State*, 440
- Oklahoma City bombing, 105, 572
- Olmstead v. United States*, 409
- Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act), 216–219
- One bite approach, 257, 260, 285
- 1-by-1 pixels, 425
- One to One Future, The* (Peppers and Rogers), 249
- Online, defined, 353
- Onsale, 12
- Openness, privacy and, 414
- Open Net Initiative, 449–450
- Open relays, 285
- Open source movement, 67, 296, 310, 316
- Operation Slam Spam, 264
- Opt in/out, 14, 47, 285
- Oregon, 118
- Organization of American States (OAS), 669, 681
- Organization for Economic Cooperation and Development (OECD):
- Bribery Working Group, 684
 - consumer protection guidelines, 347
 - defined, 432
 - democracy, principles for electronic, 621
 - e-government, 594
 - Financial Action Task Force (FATF), 685
 - global law enforcement, 669, 684–685, 687
 - history of regulation of illegitimate conduct in cyberspace, 189, 190
 - principles, 427, 428, 621
 - privacy, 413, 414, 432, 642–643
 - statistics on access, 524–525
- Organizations:
- cyberterrorism and, 167–168
 - First Amendment, and discrimination, 410
- Original data evidence, defined, 402
- Orwell, George (1984), 301
- OSI layer implementation, 738, 739
- Over-the-air (OTA), 738, 739, 783–784
- PACER (Public Access to Court Electronic Records) system, 44
- Pacifica* decision (“Seven Dirty Words”), 476
- Packet radio networks, 784
- Pagers, 784
- Paine, Thomas, 465
- Palladium, 508
- Palm, 253
- Panavision v. Toepfen*, 9, 69, 633–634
- Paperwork Reduction Act of 1995, 584
- Pasquinelli, Matteo, 312, 314
- Passive Web sites, 35
- Passport, Microsoft, 494, 495, 508, 511
- Password(s):
- defined, 842
 - guidelines for improving effectiveness of, 843
 - recovering, 368–371
- Patents, 11–12, 65, 91
- PATH variable, 774
- Patient Rights Clearinghouse, 557
- PATRIOT Act. *See* USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism)
- Pavlovich v. Superior Court*, 35–36
- PayPal, 237, 255, 340
- Peer-to-peer (P2P), 91, 320
- Perishability, 741–742
- Perry, William, 169
- Persistent cookies, 425, 433
- Personal identification number (PIN), 331, 652, 701
- Petite policy, 115
- PGP. *See* Pretty Good Privacy (PGP)
- Pharmatrak, Inc., In re*, 218, 805
- Philippines legal system, 120–121
- Phishing, 255, 256, 285, 486, 545, 706
- PHR. *See* Portable health record (PHR)
- Physical attacks, 572
- Physical channels, information leakage and, 698, 699–703
- cell phones, cameras, music players, and PDAs, 701–702
 - classic spy equipment, 702
 - disposal of media and equipment, 702–703
 - emanations, 702
 - good, old-fashioned ways, 700
 - laptops and corporate PDAs, 703
 - media, 700–701
 - office equipment, 700
 - voice and video communications, 701
- Physical evidence, defined, 402
- Physical inspection, 713
- Physical security measures, 840–841
- Physical world/analog world, defined, 173
- Pilfering, information, 753, 769–770
- PIN. *See* Personal identification number (PIN)
- Ping flooding, 150
- Pink contracts, 253, 254, 285
- PKI. *See* Public key infrastructures (PKI)
- Plagiarism, 71–72
- Planned Parenthood v. American Coalition of Life Activists*, 15
- Plea bargain, defined, 122
- Poindexter, John, 418
- Points of control, 445–447
- Policing. *See* Law enforcement, cybercrime and
- Policy(ies):
- Digital Divide and, 525
 - e-government, and procedures and infrastructures, 584–585
 - policy- or lexicon-derived methods, information leakage detection, 711
- Political groups embracing violence, 612
- Pollitt, Mark, 137
- Pollstar v. Gigmania Ltd.*, 335
- POP, 772
- POP-before-relay, 771
- Pop-up advertisements, 61
- Pornography:
- children and, 56–59
 - Communications Decency Act of 1996 (CDA), 13, 14, 45, 58–59, 447, 640–641

- cultural differences, 446
- defined, 453
- e-mail/Internet use policy and, 809–810
- forms of speech, 441
- free speech, 56–59
- Internet services providers and, 451
- search engines and, 451
- Portable health record (PHR), 537, 540–541, 558
- Portable secure environments, 717–718
- Port of Houston, denial of service attack, 118
- Post office protocol (POP), defined, 784
- Power supply, uninterruptible (UPS), 835
- Precedence, 741–742, 784
- Preponderance of the evidence, defined, 122
- Pretty Good Privacy (PGP), 331–332, 362, 366, 367, 368
- Preview window, 285
- Price competition, international, 44
- Priceline.com, 12
- Prima facie evidence, defined, 47
- Privacy, 407–433
 - banking records, 412
 - Chief Privacy Officers (CPOs), 428–429
 - children's, 412–413
 - common law, 410–411
 - constitutional, 408–410
 - consumer Internet privacy, 421–427
 - credit reports, 412
 - cultures of nations and, 195
 - czars, 642
 - definitions, 408, 433, 587, 660
 - digital id and, 482–485
 - electronic surveillance and, 234–236
 - Federal Trade Commission (FTC), 429–431
 - government and cyberterrorism, 164–167
 - government records, 412
 - information (*see* Information privacy)
 - international issues, 638–649
 - cross-border data flow, 415–416
 - EU Privacy Directive, explained, 643–644
 - laws, 413–415, 638–643
 - model contract clauses, 645–647
 - Safe Harbor compliance, explained, 644–646
 - technological responses to privacy protection, 647–649
 - threats to privacy, posed by Internet, 639–641
 - view of privacy, 642–643
- law(s):
 - basics, 408–411
 - international, 413–416, 638–649
 - state workplace statutes, 806–807
 - U.S., 412–413
- law enforcement, balancing privacy and, 416–419
 - business issues under wiretap laws, 418–419
 - ECPA (Electronic Communications Privacy Act of 1986), 216, 416, 417, 418, 419, 432
 - FISA (Foreign Intelligence Surveillance Act of 1978), 416, 417–419, 432
- legal tenets, 411
 - access, 412
 - choice, 412
 - notice, 411
 - security, 412
- medical and health insurance records, 412
- overview/introduction, 13–14, 407–408, 431–432
- policy fundamentals, 427–431
- principles of fair information practices:
 - accountability, 414–415
 - collection limitation, 413
 - data quality, 413
 - individual participation, 414
 - openness, 414
 - purpose specification, 413
 - security safeguards, 413
 - use limitation, 413
- tort concerns, 803
- trustmarks, 429
- workplace issues, 419–421
 - e-mail policies, 803, 806–807, 821
 - employee privacy policies, 420–421
 - state workplace statutes, 806–807
- Private censorship, 450–452
- Private key, 587
- Private key infrastructure (PKI), 650
- Privilege:
 - escalating, 753
 - least privilege concept, 346
- Proactive measures, 346
- Probable cause, 410
- ProCD, Inc. v. Zeidenberg*, 24, 216, 335, 338, 343
- Procedural powers, 679–680
- Prohibition, 43
- PROLOK, 341–342
- Prosecutor role, justice system, 98–102
- Prosser, William, 410
- Proximity-release door openers, 841
- Proxy computers, 260
- Proxy servers, 446, 453
- Pseudonyms, 465–466
- PSINet, 253
- "Public, the" (as a term), 226
- Public access pathways, 762–763, 773–775
- Public information, versus private information, 75–76
- Public key algorithms/systems, 332, 361, 580, 587, 650–653, 773
- Public key infrastructures (PKI), 332, 580, 650–653, 773
- Public sector:
 - e-mail/Internet use policies, 817
 - reform, 595
- Publishing:
 - e-government and, 565–566, 587
 - identity, 503, 511
- Pure cyberterrorism, 138
- Purposeful availment, 265
- Purpose specification, privacy and, 413
- Quaid Software, Ltd., 230, 341–342
- Quality of service (QoS), 784
- Quantitative national differences, 525
- Quantum computing, 580
- Quicksilver, 464, 470
- Race. *See* Demographic groups and Internet/technology use
- Race conditions, vulnerability category, 755
- Rachels, James, 74–75
- Radicati, Sara, 278
- Radio frequency identification devices (RFID), 784

- Radio networks, packet, 784
 Radios, line-sight, 783
 Radio technology, software defined, 778
 RADIUS/LEAP, 769
 RAID (redundant arrays of independent disks), 835
 Ralsky, Alan, 252
 RAM, trace evidence in, 386–388
 RAMKEY program, 341
 Raptor, 766
 Rasmussen, Michael, 158
 RAT backdoors, 770
 Rawls, John, 56
 Raymond, Eric, 310
 RC4, defined, 784
 RCFL (Regional Computer Forensic Laboratory), Dallas, 397
Real/Networks, Inc. v. Streambox, Inc., 228
 Realspace, 196
 Reasonable doubt standard, 122
 Recording Industry Association of America (RIAA), 71, 228, 231, 232, 424
 Record(s):
 accessibility requirements, online contracts, 332–333
 employee, 821
 health (*see* Medical records)
 retention requirements, online contracts, 333
 Red Cross, 611
 RedDot Solution's Content Management Server, 774
 Redundant arrays of independent disks (RAID), 835
 Refund policy, 21
Register.com, Inc. v. Verio, Inc., 23, 214–215, 222, 336, 337
 Registration, domain name, 7–8
 Regression testing, 402
 Reidenberg, Joel, 649
 Relevance, Digital Divide and, 518–519
 Remailer/reamailer software, 478
 Remote control, information leakage and, 705
Reno v. ACLU, 13, 14, 58, 59, 265, 447, 641
 Reputation service, 504
Res ipsa loquitur, doctrine of, 23
 Resistance to jamming, 741
 Retention monitoring, 710
 Reverse engineering, 210, 229–231, 340–344
 RIAA. *See* Recording Industry Association of America (RIAA)
 Ridge, Tom, 132, 135
 RIPE, 612
 RMA (revolution in military affairs) and asymmetric response, 150–151
 Roberts, Alasdair, 605
 Roberts, Julia, 10
Robotic Vision Systems v. Cybo Systems, Inc., 21
 Robots, 40–41. *See also* Bots/cyberbots
Roe v. Wade, 73, 235
 ROI of identity solutions, 505–506
 Room, clean:
 leakage prevention, 714
 reverse engineering, 341
 Room shielding, 841
 Roosevelt Dam, 132, 133
 Root server, 69
Rosenfeld v. Zemeck, 329
 Rosh, Mark, 166
 Rosser, Kevin, 154
 Royal Canadian Mounted Police, 188
 RSA Security, 331–332, 773
 RSN (robust security network), 769
 RTMark, 309
 Rumsfeld, Donald, 170
 Russia, 150, 191, 681
 Safeguards, basic security, 833–835
 Safe Harbor, 5, 7, 415–416, 433, 639, 644–646
 SafeSearch, Google, 451
 Sale of goods law, 344–347
 Salomon Smith Barney, 27
 Salvation Army, 16
 SAN (storage attached network) solution, 397–398
 SANs (storage area networks), 400
 SANS (SysAdmin, Audit, Network, Security) Institute, 157, 168
 Satellite, wireless systems with communication via, 734–735
 Satellite earth terminals, 734
 Saudi Arabia, 442, 443, 449
 SCA. *See* Stored Communications Act (SCA)
 SCADA systems, 134, 135, 144, 157, 159, 173
 Scanning, 753
 Scelson, Ronald, 244, 252, 253, 254, 256, 275–276
 Schmidt, Howard, 136
 Schumaker, Charles, 275
Schumann v. Anheuser-Busch, Inc., 800
 Scientific Working Group for Digital Evidence (SWGDE), 378
 Scurry County, Texas, voting problem in, 89
 Seal of approval programs, 429
 Search engines, 63–65, 451
 Search/seizure, 197
 Search warrant, federal, 98
 Secret key, 588
 Secret system, 834
 Secure Digital Cards, 540
 Secure Digital Music Initiative Foundation (SDMIF), 228
 Secure set identifier (SSID), 784
 Secure socket layer (SSL), 463, 478, 739
 Securities and Exchange Commission (SEC), 17, 27
 Security:
 computer, 81–84
 legal protection of, 82
 moral legitimacy of rights of, 82–83
 employee liabilities related to, 25–26
 of information, defined, 784
 privacy and, 412, 413
 as a term, 81–82
 Security system, guidelines for comprehensive, 831–850
 comprehensive security plan, 844–847, 850
 disasters, preparing for/recovery, 847–849, 850
 identification of basic security safeguards, 833–835
 identification of computer emergency response team services, 843–844
 identification of general security threats, 835–836
 internal/external threats and vulnerability, 836
 potential computer and network disasters, 835

- identification of security measures and enforcements, 838–843
 - backups, 838
 - biometric security measures, 838, 839
 - callback modems, 838–839
 - electronic rackers, 841
 - firewalls, 838, 839–840
 - identification badges, 841
 - intrusion detection systems (IDS), 838–839, 840
 - physical security measures, 840–841
 - proximity-release door openers, 841
 - room shielding, 841
 - smart cards, 841
 - software security measures, 842
 - token, 841
- intentional threats, 836–838, 850
- overview/introduction, 831–832, 849
- terms defined, 849–850
- unintentional threats, 850
- Security task force, 832–833, 850
- SeeBeyond, 509
- Seescandy test, 473, 474
- Sega Enterprises Ltd. v. Acolade, Inc.*, 229
- Self-defense, 107
- Self-help response to cybercrime, 110
- Self-insured, 33
- Sentencing, criminal justice system, 113–114, 122
- Service delivery, 567, 588
- Service mark, 47
- Service set identifier (SSID), 758
- Session cookies, 425, 433
- Session server, 503
- Session service, 503
- Session token, 503
- SettleOnline, 39
- “Seven Dirty Words” (*Pacifica* decision), 47
- Sex.com, 57
- Sex discrimination/harassment, 800–803, 814
- Sexually explicit content, 445. *See also* Pornography
- SHA-1 hash, 402
- Shattuck v. Klotzbach*, 331
- Shetland Times v. Shetland News* (Scotland), 40
- Shrink-wrap agreements versus clickwrap, 24, 47, 334–337
- Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 223
- Siebel, 474
- Signatures. *See* Electronic/digital signatures
- Silicon Investor, 472
- SIM (subscriber identification module), 784
- Simple object access protocol (SOAP), 491
- Singapore, 445, 449
- Single click patents, 12, 494, 658–659
- Single sign-on (SSO), 494, 495
- Slammer worm, 33, 150, 157
- SLAPPs (strategic lawsuits against public participation), 166
- Smart cards, 462, 463, 841
- SmartFilter, 450
- Smart Media, 540
- S/MIME (Secure Multipart Internet Mail Extension), 720
- Smith v. Hoocy*, 105
- SMTP authentication, 770
- Smurf attacks, 573
- Smyth v. Pillsbury Co.*, 235, 796
- Social engineering, 545, 691, 756, 784
- Social networking and contact management sites, information leakage and, 704–705
- Society for Human Resource Management (SHRM), 419
- Socks servers, 464, 478
- Soft Effects test, 634
- Software:
 - access codes, 842
 - contractual restrictions on use of, 340–344
 - copyright preemption, fair use, and reverse engineering, 340–344
 - data encryption, 842 (*see also* Encryption)
 - defined, 173
 - electronic transaction securities, 842–843
 - passwords, 842, 843
 - patents, 657–659
 - security measures, 842
 - terminal resource security, 842
- Software defined radio technology, 778
- SOMTC (Senior Officials Meeting on Transnational Crime), 663
- Sonny Bono Copyright Term Extension Act (1999), 6–7
- Sony, 255
- Sophos mail server, 770
- Sora, Orlando, 274
- Source code, 316
- South Africa, 190, 651, 673
- South America, 820
- Soviet Union, former, 11
- Spacey, Kevin, 10
- Spam, 243–286
 - Anti-Spam Coalition, 270
 - antispammers, 254
 - balanced viewpoint, 247–248
 - copyright and, 441, 446
 - closed loop marketing, 249–250
 - costs of, 245–247, 442–443
 - crime and, 255–264
 - defining, 91, 271–275, 442, 453
 - commonly used definitions, 271–273
 - permissive definitions, 273–275
 - restrictive definitions, 273
 - effect of legislative counterattack, 275–277
 - antispammer perspective, 276
 - business perspective, 276–277
 - government perspective, 275
 - spammer perspective, 275–276
 - states’ perspective, 277
 - enforcement and prosecution, 264–275
 - federal CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003), 20, 62, 248, 258–263, 264–271, 276, 285, 482
 - Commerce Clause in U.S. Constitution, 266–268
 - do-not-spam lists, 261–262
 - First Amendment, 264–265
 - implementation questions, 260–261
 - jurisdiction and due process, 265–266
 - list restrictions, 262–263

- Spam (*Continued*)
- other prosecutions, 269–271
 - provisions, 259–260
 - state legislation and, 264–271
 - Trespass and Nuisance claims, 268–269
 - first law school course on, 248
 - free speech and, 61–62
 - global perspective, 277–281
 - European legislation, 278–279
 - growing international action, 279–281
 - movement offshore, 277–278
 - industry self-regulation, 263–264
 - “junk mail,” 244–245
 - legal counterattack, 256–258
 - “no Spam in Heaven” marketing, 251–252
 - origin of term, 249
 - overview/introduction, 19–21, 243–248, 281–285
 - reasons for, 249–252
 - spammers, 250–255, 459
 - “spam” versus “SPAM,” 248
 - state and local legislation, 257–258
 - terms defined, 285–286
 - war on spam, 256–257
- Specht v. Netscape Communications Corp.*, 23, 337, 344
- Spectorsoft.com, 80
- Spheres of authority, 609
- Spiders, 40–41
- Spinello, Richard, 57, 61, 77, 80
- Spitzer, Eliot, 270
- Sponsors, cyberterrorism, 152–155
- Spoofing, 255, 286, 459, 573, 769
- Sportinggoods.com, 69
- Springfield Hydroelectric Company v. Copp*, 29
- Springsteen, Bruce, 10
- SpyBuddy, 169
- SpyCop, 169
- Spy-patrol.com, 80
- Spy software, 80
- SQL Slammer, 157
- SquareTrade.com, 39
- SSL. *See* Secure socket layer (SSL)
- SSO. *See* Single sign-on (SSO)
- Stallman, Richard, 67, 299, 310
- Stalking, 117, 122
- State(s), U.S.:
- cybercrime law, 116–117
 - databases, and information privacy, 79–80
 - relationship between state and federal criminal justice systems, 114–115
 - UCITA (bomb shelter legislation), 347
 - workplace privacy statutes, 806–807
- State Farm Mutual Auto. Ins. Co. v. Bockhorst*, 327
- State of Washington v. Heckel*, 267, 272
- Stateside Associates, 557
- State-sponsored attacks, 572
- State Street Bank v. Signature Financial Group*, 12, 658
- State v. Schwartz*, 118
- Statistical methods, leak detection, 711
- Statute of Frauds, 323, 329
- Statutes, Web sites for obtaining, 65
- Stealing versus copying files, 118
- Steganography, 371–376
 - coping with, 375–376
 - demonstration, 372–375
 - file recovery, 375
 - manual methods of determining content, 376
- Stegdetect, 376
- Stella D’Oro Biscuits, 10
- Steven Jackson Games, Inc. v. United States Secret Service*, 218
- Sting, 10
- Storage Attached Network solution (SAN), 397–398
- Stored Communications Act (SCA), 216, 219–221
 - backup files, 220–221
 - temporarily stored communications, 221
- Stranger danger, 107
- Strict Effects test, 634
- Student plagiarism, 71–72
- Subpoenas seeking identity of anonymous speakers, 471–473
- Subscriber identification module (SIM), 784
- Suck.com Web sites, 16
- Sudan, 153
- Sui generis* protection, 657
- Sun Microsystems, 491, 509
- Sunstein, Cass, 476
- Supremacy Clause of the U.S. Constitution, 342
- Surveillance/investigation, 164–167. *See also* USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism)
- Swallow factories, 314
- Swap files, trace evidence in, 388–389
- SWIFT (Society for Worldwide Interbank Financial Telecommunication), 615
- Symbolic links, 755
- Symmetric, defined, 588
- Symmetric ciphers, 361
- Tactical media, 305
- Tactics, 745
- Talley v. California*, 466
- Target, defined, 785
- Targets of evaluation (TOE), 785
- Target wireless operations, 751–752
- Task force, security, 832–833, 850
- Taxation, 19–21, 600
- Taxonomy, defined, 785
- TBG Insurance Services Corp. v. Superior Court*, 235–236
- TDEA (triple data encryption algorithm), 581, 583
- Technical solutions, cyberterrorism, 146
- Technological American Party (TAP)*, 301
- Technological literacy, 518
- Technological responses to privacy protection, 647–649
- Technology and the state, 593–594
- Telstra (Australian telecom company), 10
- Tempest, 702
- Temporal attacks, 746
- Teoma, 64
- Terminal resource security, 842
- Term-paper-time.com, 72
- Terms, unusual/onerous, 337–338
- Terms of Use provisions, 21–22, 24, 47, 214–216, 240

- Terrorism:
- computer/Internet systems and (*see* Cyberterrorism)
 - financial institutions and, 236–237
 - 9/11, defined, 172
 - post-9/11 world, 33, 129, 131, 154–155, 165, 170, 198–199, 482
- Terrorism Information Awareness (TIA), 166
- Tethered mobility, 785
- Thailand, 191
- Theofel v. Farey-Jones*, 220–221
- Third-party cookies, 425, 433
- Thompson, Loren, 151
- Threats:
- acts versus, 138
 - to confidentiality, 577
 - defined, 199, 558
 - exaggerated, 133–135
 - external, 544–546, 836
 - general security, 835–836
 - identifying, 544, 835–836
 - intentional, 836–838, 850
 - internal, 545, 836
 - to privacy, posed by Internet, 639–641
 - traditional (three areas), 736
 - unintentional, 850
- TIBCO, 509
- Tiberino v. Spokane County*, 817
- Ticketmaster* case, 335, 336
- Tien, Lee, 477
- Time division multiple access (TDMA), 785
- Time Warner, 40, 44
- TISM (Trust Information Sharing Network for Critical Infrastructure Protection), 599
- TOC (transnational organized crime) convention, 675, 676
- Toeppen*, 9, 69, 633–634
- Token:
- session, 503
 - transmission device, 841
- Tools, cyberterrorism, 146–148
- Tort(s), 48, 826
- appropriation, 411
 - disclosure, 411
 - false light, 411
 - intrusion, 411
- Total Information Awareness, 418
- Total News, framing case against, 40
- Toussaint v. Blue Cross & Blue Shield of Michigan*, 799
- Toysmart.com, 431
- Toys R Us, Inc. Privacy Litigation, In re*, 221
- Trace evidence:
- in RAM, 386–388
 - in swap and hibernation files, 388–389
 - in unallocated space, 389–392
- Trackers, electronic, 841
- Trademark(s):
- defined, 48, 91
 - dilution of, 8–9
 - as domain names, and cybersquatting, 4 (*see also* Cybersquatting; Domain names)
 - infringement, 40
 - law, 65
- Trademark Counterfeit Act (1984), 42
- Trade secrets:
- defined/explained, 210–211, 225–226, 240, 826
 - e-mail and Internet use policy, and protection of, 808–809
 - Trade Secrets Act (TSA), 225
- Tragedy of the commons, 602
- Transaction processing, 567, 588
- Transfer control protocols (TCPs), 144
- Transmission control protocol (TCP), 173, 573
- Transmission security (TRANSEC), 749, 785
- Transparency International, 606, 611
- Transport information, high risk of, 619–620
- Treaties:
- Convention on Cyber-Crime, 676–680
 - computer-related offenses, 677–678
 - content-related offenses, 678–679
 - copyright infringement, 679
 - Council of Europe, defined, 122
 - countries signing, 121, 190
 - defined, 199
 - jurisdiction, 679
 - procedural powers, 679–680
 - encryption exportation regulation; United States law and international treaties, 650–651
 - enforcement, 605
 - first international treaty on criminal offenses committed against or with help of computer networks, 155
 - mutual legal assistance (MLA), 120, 121, 673, 676, 680, 683, 684, 691
 - nations opting out of, 605
- Trenchard, John, 465
- Trespass, 213–214, 240
- Trial by jury or trial by judge, 103–105
- Triple bottom line, 622
- TRIPs (Trade-Related Aspects of Intellectual Property Rights), 189, 655
- Tripwire, 764
- Trojans/Trojan horses, 118–119, 445, 756, 759, 785
- Trust domain, 511
- Trust-E, 78–79
- TRUSTe, 428, 429
- Trusted agents, attack via, 760–762, 772
- Trusted third party, 653
- Trustmarks, 429, 433
- Trust services, 503, 511
- Tumbleweed Communications, 12
- Tunneled protocols, information leakage and, 705
- Turkey, 631
- Turkle, Sherry, 458
- Turner, Ted, 10
- 24/7, defined, 172
- 2themart, 472
- UBE (unsolicited bulk e-mail), 272, 286
- UCBE (unsolicited commercial bulk e-mail), 272, 286
- UCITA. *See* Uniform Computer Information Transactions Act (UCITA)
- UEMS (unsolicited electronic mail solicitations), 272
- UETA. *See* Uniform Electronic Transactions Act (UETA)

- Unallocated space:
 defined, 402
 trace evidence in, 389–392
- Unconscionability, doctrine of, 321, 339–340
- UNICODE/ASCII, 380, 381, 382, 383, 392, 506
- Uniform Commercial Code (UCC), Article 2, 324
- Uniform Computer Information Transactions Act (UCITA), 324, 327, 345, 346–347, 349, 352
- Uniform Domain-Name Dispute-Resolution Policy (UDRP), 9
- Uniform Electronic Transactions Act (UETA), 324, 326, 348
- Uniform resource identifiers (URIs), 497
- Unintentional threats, 850
- Uninterruptible power supply (UPS), 835
- Union-represented employees, 816
- United Kingdom, 119, 185, 278, 483, 599, 681
- United Nations:
 censorship standards, 443
 Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce, 324, 325, 349, 654
 Conference on Trade and Development (UNCTAD), 522, 525
 Contracts for the International Sale of Goods (CISG), 36
 Convention against Transnational Organized Crime (TOC) Convention, 668, 674–675
 cybercrime (1990), addressing in, 189
 cyberterrorism, 154–155
 Digital Divide, 522, 523–524
 General Assembly Resolution, 687
 Office of Drug Control and Crime Prevention (UNDCP), 669, 683
 spam and, 246, 280–281
 statistical indexes, 523–524, 594
 Universal Declaration of Human Rights, 413
United States et al. v. American Library Association, 15
United States of America v. Sami Omar Al-Hussayen, 141
United States v. Aluminum Company of America (ALCOA), 632
United States v. American Library Association, 63
United States v. Councilman, 216
United States v. Czubinski, 106
United States v. Hsu in footnote on 226, 226, 227
United States v. Lange, 226
United States v. Slanina, 236
United States v. Yang, 227
Universal City Studios, Inc. v. Corley, 104
Universal City Studios, Inc. v. Reimerdes, 40, 228
 Universal Description, Discovery, and Integration (UDDI), 491
 Universal Health Care Action Network, 557
- UNIX, 169, 363, 388, 389, 390
 five types of, 752
- Unsolicited bulk e-mail (UBE), 785
- Unsolicited commercial e-mail (UCE), 257
- URI. *See* Uniform resource identifiers (URIs)
- Uruguay Round Agreement, 189, 655
- USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism):
 acronym defined, 42, 164, 198, 206, 240
 businesses, and government spying, 236–238
 congressional review of, 164, 283, 416–417
 corporate spying and, 206, 217, 219, 236–238
 criticism/challenges to, 164–165, 166, 484
 defined, 240
 difficulty of using/onerous mechanisms of, 401
 Electronic Communications Privacy Act (ECPA) and, 237–238, 812–813
 Foreign Intelligence Surveillance Act (FISA) and, 416–417, 418–419, 649
 hacktivism and, 305
 post-9/11 passage of, 164, 198, 470, 484, 648
 privacy and, 639, 648
 provisions, 42–43, 164–165, 167, 198, 217, 470, 648–649
 Web site for obtaining text of, 74
- USA Today*, 40
- U.S. Bancorp Piper Jaffray, 27
- USB Key Chain Drives, 540
- U.S. Copyright Felony Act, 185
- U.S. Copyright Office, defined, 48
- Use limitation, privacy and, 413
- User datagram protocol (UDP), 573, 577
- U.S. Financial Services Modernization Act, 75
- U.S. laws covering electronic transactions, 324–325
- U.S. Patent and Trademark Office (PTO), defined, 48
- USPS (U.S. Postal Service), 255
- U.S. Rehabilitation Act, 519–520
- U.S. v. Eisenberg*, 323
- U.S. v. Grande*, 323
- U.S. v. Hicks*, 101
- U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT), 165
- U.S. v. Middleton*, 223
- U.S. v. \$734,578.82 in U.S. Currency*, 42
- U.S. v. Simmons*, 815
- Utilitarianism, 55–56, 67–68, 91
- Validation of digital forensic tools, 377–384
- Validity, 22–23, 24
- Value chain, IT system design, 614
- Vatis, Michael, 130
- Vault Corp. v. Quaid Software, Ltd.*, 230, 341–342
- Verio case, 23, 214–215, 222, 336, 337
- VeriSign, 331–332
- Verizon, 232, 270, 338, 424
- Victim(s):
 liability and, 28–31
 sentencing and, 113
 victim impact statement, 123
- Vigilante action, 110–111, 614
- Violence:
 political groups embracing, 612
 terrorism (*see* Cyberterrorism)
 workplace, and e-mail/Internet use policies, 821–822
- Viral marketing, 260
- Virtual force, versus physical force, 107
- Virtual identities, 458
- Virtual identity document, 500
- Virtual local area network (VLAN), 752, 759, 760, 763, 774, 776–777, 785
- Virtual private network (VPN), 769, 773, 785
- Virtual sit-ins, 306, 316
- Virtual world/digital world/cyberspace, defined, 172

- Viruses/worms/malware:
 defined/explained, 122, 445, 785, 836
 indications of infection, 838
 information leakage and, 706
 overview/introduction, 26–27
 security, censorship, and points of control, 445, 446
 state laws, 116–117
 untenable assumptions of identity, and, 459
 worm versus virus, 445
- Visa, 29, 30
- VLAN. *See* Virtual local area network (VLAN)
- Voice over Internet Protocol (VoIP), 469
- VOMIT (Voice over Misconfigured Internet Telephony), 701, 720
- Voting:
 electronic (*see* E-voting)
 information for, 595
 rights, 85
- VPN. *See* Virtual private network (VPN)
- Vulnerabilities, 145–146, 577, 616–619, 749–756, 836
- W.32.Bugbear virus, 157, 159
- W3C, 491
- Walker, Jay, 659
- Walker Digital, 659
- Wall Street Journal* Web site, 634
- Wal-Mart, 10, 309, 506
- Waltz, Edward, 725
- WareZ, 100, 720
- Warfare, 151. *See also* Electronic warfare; Information warfare (IW)
- Warrant(s), 410
- Warranties, 345–347
- Wartime, anonymity during, 469–470
- Washington Post Co., et al. v. Total News*, 40
- Washington state, 34, 62, 267, 270, 272, 431
- Wassenaar Agreement, 651
- Watchtower Bible and Trust Society v. Village of Stratton*, 467–468
- Weather, 597
- Web, information leakage and, 704
- Web-beacons, 425
- Web browsers, and privacy, 422
- Web bugs, 425–426, 433
- Web-cams, 411
- Web log analysis, 712
- Web publishing, information leakage and, 705
- Websense Enterprise, 450
- Web services, 490–491, 511
- Web sites:
 defacements, 308
 estimates of number of, 63
- WEP, 752, 757, 758, 767, 769, 778, 785
 wired equivalency privacy, 785
 wired equivalency protocol, 757
 wireless encryption protocol, 752, 767, 769
- Wesley Coll. v. Pitts*, 218
- West, Darell, 520
- Whistle-blowing, 824
- White House Web site, 70, 139
- White list, 286
- WHOIS database, 214, 336
- Wifi Protected Access (WPA), 752, 778, 785
- Wikipedia, 67
- Windows:
 encrypted file system, 365–366
 swap/hibernation files, 388
- WIPO. *See* World Intellectual Property Organization (WIPO)
- Wired equivalency privacy, 785
- Wired equivalency protocol, 757
- Wireless encryption protocol, 752, 767, 769
- Wireless information warfare (WIW), 723–786
 defensive information operations (information assurance), 748–749
 defined, 725–726, 785
 offensive malevolent acts, 744–748
 content attacks, 746
 cryptographic attacks, 747–748
 direct, or internal, penetration attacks, 746
 effect, 745
 ethics and legality, 745
 functions, 744–745
 indirect, or external sensor attacks, 746
 invasiveness, 745
 motive, 745
 tactics, 745
 taxonomy of attack operations, 745–747
 techniques, 745
 temporal attacks, 746
 overview/introduction, 723–725, 777–779
 secure communications and system design, 743–744
 terms defined, 779–786
 unique aspects of, 736–743
 military-unique system requirements, 741–742
 performance measures and key design trade-offs, 740–741
 traditional threats, three areas, 736
 why is wireless security different, 737–740
- Wireless information warfare (WIW) in practice, 749–777
 example attack, remote attack on wireless network (VLAN hopping), 756–763
 attack via public access pathways, 762–763
 attack via trusted agents, 760–762
 diagram, 757
 example defenses, 763–777
 attacker identification, 772
 against attack via public access pathways, 773–775
 from attack via trusted agents, 772
 firewall, 765–766
 host-based intrusion detection system (h-IDS), 763–765
 incident response, 775–776
 against information pilfering, 769–770
 against malicious code introduction, 770–772
 against remote doctor offices, 772–773
 against VLAN hopping, 776–777
 for wireless networks, 766–767
 example vulnerabilities of a suburban hospital, 749–756
 security measures for the hospital, 750–751
 target wireless operations, 751–752
 VLAN operations and servers, 752
 wireless attacks, 753–756

- Wireless information warfare (WIW) taxonomies, 726–733
 - classification by
 - confidentiality/integrity/availability (CIA), 727–732
 - corruption, 728
 - detection, 730
 - disruption, 727
 - exploitation, 728–729
 - response, 730
 - classification by domain of information aggression, 727, 728
 - classification by exploitation and attack/defense, 732–733
 - deception, 733
 - electronic warfare, 733
 - information corruption, 733
 - security, 733
 - relationship to asymmetric warfare, 731–732
- Wireless local area network (WLAN), 786
- Wireless modems, 786
- Wireless networks:
 - information leakage and, 705
 - taxonomies of, 733–736
 - mobility classifications, 735–736
 - network architecture classifications, 734–735
- Wireless security implementation, 786
- Wireless services, interrelationships among (diagram), 730
- Wireless technology, employee use of, 798
- Wiretap Act (Omnibus Crime Control and Safe Streets Act of 1968), 216–219
- Wiretapping, government, 410. *See also* USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism)
- Wizards of OS, 312
- WLAN, 750, 751, 778
- Woolley v. Hoffmann-La Roche, Inc.*, 799
- Work for hire, 213
- Workplace boundaries, blurring of, 795–797
- Workplace laws, foreign, 819–821
- Workplace monitoring, electronic, 811–812, 825
- Workplace policies. *See* Employer e-mail/Internet use policies
- World Bank, 594–595
- WorldCom, 276, 800
- World Intellectual Property Organization (WIPO), 5, 10, 48, 604, 654–657
- World Trade Organization (WTO), 155, 604, 649, 654, 655
- Worldwide perspective, cyberterrorism, 154–155. *See also* Cyberterrorism
 - World-Wide Volkswagen Corp. v. Woodson*, 632
 - World Wide Web (a.k.a. Web), defined, 173
 - World Wrestling Federation, 10
 - Worm versus virus, 445. *See also* Viruses/worms/malware
 - WPA. *See* Wifi Protected Access (WPA)
 - WPISP (OECD Working Party on Information Security and Privacy), 599
 - Wrongful discharge, 814
 - WSDL (web services description language), 491, 503
 - WSIS (World Summit for the Information Society), 601, 612, 621
 - WTO. *See* World Trade Organization (WTO)
 - X12N, ANSI, 541–542, 555, 558
 - Xanadu, 300
 - XML (extensible markup language), 491, 503, 506
 - XML Schema, 503
 - XNS (extensible name service), 494, 495, 496, 497, 498, 499, 501, 502, 504, 510
 - XNS Negotiation Service, 501
 - XNSORG, 494, 508
 - XRI (extensible resource identifier), 496, 497, 498, 510
 - XRI data interchange (XDI), 496, 502, 511
 - XSS (cross-site scripting), 762, 763, 774, 780–781
 - Yahoo!
 - anonymity and, 12
 - China, 449
 - denial of service attacks, 26, 836
 - domain name disputes, ICANN's resolution process, 10
 - domination of, 44
 - GeoCities, 430
 - Nazi memorabilia decision (*Yahoo! v. La Ligue Contre Le Racisme et L'Antisemitisme*), 37, 42–631, 636–368
 - spam and, 284
 - Yes Men, The, 309
 - Youth International Party Line*, 301
 - ZD.net, 836
 - Zefer Corporation, 223–224
 - Zeidenberg (*ProCD, Inc. v. Zeidenberg*), 24, 216, 335, 338, 343
 - Zenger, John Peter, 465
 - Ziff Davis, 30
 - Zippo sliding-scale standard (*Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*), 34–36, 632–633
 - Zombie computers, 255, 256, 286
 - ZoneLabs personal firewall, 546