Cyberlaw: text and cases

. Selections

Authors: Gerald R. Ferrera, Stephen D. Lichtenstein, Margo E. K. Reder, Robert C. Bird, Christine N. O'Brien

Persistent link: http://hdl.handle.net/2345/bc-ir:103474

This work is posted on eScholarship@BC, Boston College University Libraries.

Mason, Ohio: Thomson/South-Western/West, c2004
Second Edition

CyberLaw

Text and Cases

Gerald R. Ferrera
Bentley College

Stephen D. Lichtenstein
Bentley College

Margo E. K. Reder
Boston College

Robert C. Bird
Seton Hall University

William T. Schiano
Bentley College

THOMSON
SOUTH-WESTERN WEST

Australia • Canada • Mexico • Singapore • Spain • United Kingdom • United States
In loving memory of Susan and Raymond Ferrera and Karna and Lawrence McCabe

—GRF

For my wife, Cindy, our children Jeff and Julie, and my parents, Max and Frances

—SDL

For my family, with gratitude for your encouragement throughout this project

—MEKR

For my father, Dennis, and my mother, Lois

—RCB
About the Authors

GERALD R. FERRERA received a B.S. from Boston College, an M.S. in taxation from Bentley College, and a J.D. from New England School of Law. He has co-authored texts in business law and legal environment and has written numerous law review articles. He was granted the Gregory H. Adamian Law Professorship, the first endowed chair of the law department at Bentley College. In 2002 he was awarded the Senior Faculty Award of Excellence from the Academy of Legal Studies in Business.

Publication awards include the Ralph C. Hoeber Award given by the Academy of Legal Studies in Business, numerous Bentley College publication awards, and the Bentley College Scholar of the Year Award. Teaching awards include the Charles M. Hewitt Excellence in Teaching Award granted from the Academy of Legal Studies in Business, and from Bentley College, the Gregory H. Adamian Teaching Award and the Innovative Teaching Award. He is the founder and executive director of the Bentley College CyberLaw Center. He was president of the North Atlantic Regional Business Law Association and currently serves on the Executive Committee and the board of editors of the Business Law Review. He was chair of the Bentley College Law department and is presently a research fellow at the Center for Business Ethics at Bentley College. He is also a member of the Massachusetts and federal bars.

STEPHEN D. LICHTENSTEIN has a B.S. from Boston College, a J.D. from Suffolk University Law School, and a Certificate in Mediation. He has authored and co-authored numerous law review articles on many business law-related topics. Publication awards include a Ralph C. Hoeber Award given by the Academy of Legal Studies in Business. He is the founder of the Bentley Consumer Action Line, a community-service learning program under the auspices of the Massachusetts attorney general’s office, where students mediate actual consumer complaints against businesses. He is also co-director of the Bentley College CyberLaw Center. In 2000 he received the prestigious Bentley College Adamian Award for Excellence in Teaching. Professor Lichtenstein is past president of the North Atlantic Business Law Association, and he currently serves on the Executive Committee and the board of editors of the Business Law Review. He is a legal consultant to business and individuals and a member of the Massachusetts and federal bars. Currently, he is the chair of the Bentley College Law Department.

MARGO E. K. REDER is a Lecturer in Law at the Carroll School of Management, Boston College. Her courses in the M.B.A. program focus on e-commerce and cyberspace law. She has previously served as a prosecutor and counsel for a start-up. She is past president of the North Atlantic Regional Business Law Association and currently serves on both its executive and editorial boards. Ms. Reder has contributed to a number of legal texts and authored over twenty law review articles. She is widely cited for her work in securities regulation, arbitration, employment, international transactions, and most recently in the cyberlaw field. Ms. Reder graduated from the
University of Massachusetts, London School of Economics and Political Science, and Suffolk University Law School. She is a member of the state and federal bars.

ROBERT C. BIRD received his B.S. in information systems from Fairfield University, a J.D. from Boston University School of Law, and an M.B.A. from Boston University Graduate School of Management. He is currently an assistant professor of legal studies at Seton Hall University and has taught as an adjunct professor at Fairfield University and Sacred Heart University. Mr. Bird teaches undergraduate and graduate legal courses to business students. He presently serves as a staff editor to the *Journal of Legal Studies* and the *American Business Law Journal*. Also, he is a member of the Academy of Legal Studies in Business, the North Atlantic Regional Business Law Association, and the Northeast Academy of Legal Studies in Business. His research interests include contract law, employment law, and, of course, cyberlaw.

Mr. Bird’s articles have appeared in the *Kentucky Law Review*, the *American Business Law Journal*, and the *William & Mary Journal of Women & the Law*. Besides being a two-time finalist in the Academy of Legal Studies in Business/Master Teacher Competition, he has won the Seton Hall University’s Excellence in Teaching Award for his first year in full-time teaching, spring 2001. Mr. Bird is licensed to practice law in Connecticut and New York. He has also served as a law clerk to a number of courts including the Connecticut Appeals Court, the U.S. Bankruptcy Court, and the Massachusetts Superior Court. Mr. Bird also acts as an appellate adviser on civil legal matters, authoring a victorious legal brief for the plaintiffs in *Pequonnock Yacht Club v. City of Bridgeport*, 259 Conn. 592 (2002).

WILLIAM T. SCHIANO is an assistant professor and chair of the MIS department at Bentley College. He developed and taught two graduate MIS courses, “Information Technology Management and Policy” and “Electronic Commerce in the Global Economy,” and he has written numerous articles, papers, and Harvard Business School cases. He is a VanDuyne Scholar from the Williams College Department of Economics, with other honors and awards that include participant in the 1995 Ernst & Young Foundation ICIS Doctoral Consortium and a Harvard University Fellowship.
Brief Contents

Preface, xviii
List of Cases, xxiv

1 Introduction to Cyberlaw, 1
   1 Technology and Cyberlaw, 3
   2 Jurisdiction, 15

2 Intellectual Property Issues in Cyberspace, 45
   3 Trademarks, 47
   4 Copyrights, 83
   5 Business Methods Patents and Trade Secrets, 111

3 Business and Financial Issues in Cyberspace, 149
   6 Online Contracting, 151
   7 Sales Tax in E-Commerce, 193
   8 Online Securities Offerings and Transactions, 219

4 Special Issues in Cyberspace, 255
   9 Privacy, 257
  10 Obscenity, 311
  11 Defamation, 343
  12 Internet and Information Security, 367
  13 Internet and Computer Crime, 405

Appendices, 445
Glossary, 505
Index, 513
## Contents

Preface, xviii  
List of Cases, xxiv  

### Part 1  Introduction to Cyberlaw

1 Technology and Cyberlaw, 3  
   Introduction, 3  
   History of the Internet, 4  
   History of the World Wide Web, 4  
   How the Internet Works, 5  
      - *Internet Addresses*, 5  
      - *The Language of the Internet*, 6  
      - *Accessing a Web Site*, 6  
      - *Transmitting Information*, 6  
      - *Netiquette*, 7  
   Regulation of Cyberspace, 7  
      - *Business and Individual Users*, 9  
      - *Information Security*, 10  
      - *Ping of Death*, 11  
   Business Uses of Internet Technologies, 11  
   Globalization, 12  
   Law and Cyberspace, 12  
   Summary, 13  
   Key Terms, 13  
   Manager’s Checklist, 14

2 Jurisdiction, 15  
   Introduction, 16  
   Categories of Jurisdiction, 17  
   Traditional Principles of Jurisdiction, 20  
      - *State Long-Arm Statutes and Personal Jurisdiction over a Nonresident Defendant*, 20  
      - *Application of the Due Process Clause over a Nonresident Defendant*, 21  
      - *Motion to Dismiss for Lack of Personal Jurisdiction over a Nonresident Defendant*, 23  
   Judicial History of Personal Jurisdiction, 23  
      - *Constitutional Framework for Due Process under the International Shoe Company Case*, 23  
      - *Two-Pronged Analysis for Finding Personal Jurisdiction in the International Shoe Company Case*, 24  
   Personal Jurisdiction in the Online Environment, 25
Part 2 Intellectual Property Issues in Cyberspace

3 Trademarks, 47

Introduction, 47
Intellectual Property, 48
Trademarks, 48
- Service Marks, 50
- Trade Dress as a Trademark, 50
- Registering a Trademark, Trade Dress, or Service Mark with the USPTO, 51
- Duration of a Trademark, 51

Trademarks as Distinctive: Either Inherently or Through a Secondary Meaning, 52
Julia Fiona Roberts v. Russell Boyd, 54
Trademark Infringement and Dilution, 58
- Trademark Infringement, 58

Checkpoint Systems, Inc. v. Check Point Software Technologies, Inc., 59
- Trademark Dilution, 63
A.B.C. Carpet Co., Inc., et al. v. Naeini, 64

Trademarks in Cyberspace: Cyberpiracy and Internet Technology, 67
- Anticybersquatting Consumer Protection Act (ACPA), 67
E & J Gallo Winery v. Spider Webs Ltd., 68
- Internet Technology and Trademark Infringement, 70
Playboy Enterprises Inc. v. Welles, 73
4 Copyrights, 83
Introduction, 83
Copyright Act of 1976, 86
- Subject Matter of Copyrights, 87
- Requirements for Registration in the Copyright Office, 88
- Duration of Copyright, 88
Constitutional Challenge to the Sonny Bono Copyright Term Extension Act, 88
Eldred v. Ashcroft, 89
Exclusive Statutory Rights of a Copyright Owner, 91
- Right to Reproduce the Work, 91
- Right of Distribution: Selling, Renting, or Leasing Copies, 92
- Right to Prepare Derivative Works, 93
- Right to Perform and Display Publicly a Copyright Work, 94
Theories of Liability for Copyright Infringement, 94
- Direct Infringement, 94
- Contributory Infringement, 95
- Vicarious Infringement, 95
Religious Technology Center v. Netcom On-Line Communication Services, Inc., 95
Limitations on Copyright Owners’ Exclusive Rights, 98
- Fair Use Doctrine, 98
- First Sale Doctrine, 99
- Public Domain, 99
- Other Statutory Exemptions on Copyright Owners’ Exclusive Rights, 99
Remedies for Copyright Infringement, 100
The Digital Millennium Copyright Act (DMCA), 101
- Anti-Circumvention of “Digital Locks,” 101
- Copyright and Management Systems, 101
- Trafficking in Circumvention Tools, 102
Safe Harbor for Online Service Providers Under the DMCA, 102
- Online Service Providers (OSPs), 102
Section 512 of the Digital Millennium Copyright Act (DMCA) and the Napster Case, 103
Part 3  Business and Financial Issues in Cyberspace

6  Online Contracting, 151

Introduction, 151
- Why Is Online Contracting Law Important?, 152
- History and Development of Online Contracting, 152
- Terms of E-Commerce, 153
- E-Commerce Business Models, 154
- Benefits to Consumers, 155

Fundamental Principles of Contract Law, 155
The Requirements of a Contract, 155
- Mutual Assent, 156
- Consideration, 158
- Capacity, 158
- Legality, 159
- Form, 160
- Exceptions to the Statute of Frauds’ Writing Requirement, 160

Warranties, Disclaimers, and Terms of Use, 161
- Other Terms of Use: PayPal, Inc.’s User Agreement, 163
- Disputing the Terms of Use: Comb v. PayPal, 165

The Developing Uniform E-Commerce Law: UCITA and UETA, 166
- History and Development, 166
- UCITA: A Controversial Measure, 167
- UCITA: Key Provisions, 168
- The UETA, 170

Electronic Signatures, 171
- Current Electronic Signature Legislation: E-Sign, 172

Software Licensing, 173
- Key Terms/Components of a Software Licensing Agreement, 174

Click-Wrap, Shrink-Wrap, and Browse-Wrap Agreements, 176
ProCD, Inc. v. Zeidenberg, 177
Specht v. Netscape Communications Corp., 179
E-Commerce and Insurance: Insuring Online Contracting Risk, 182
State Auto Property & Casualty Insurance Company v. Midwest Computers & More, 183
International Aspects of Electronic Contracting, 187
- UN Convention on Contracts for the International Sale of Goods, 187
- UNCITRAL Model Law on E-Commerce, 187
- EU Directive Concerning E-Commerce, 188
Summary, 188
Key Terms, 189
Manager’s Checklist, 189
Case Problems, 190
Additional Readings, 192

7 Sales Tax in E-Commerce, 193
Introduction, 194
- Taxation in Cyberspace, 195
- State Tax Jurisdiction Under the U.S. Constitution, 195
- Mail-Order Transactions, 196
National Bellas Hess, Inc. v. Dept. of Rev. of the State of Illinois, 198
Quill Corp. v. North Dakota, 201
- Physical Presence Nexus Test for E-Commerce, 204
- Internet Tax Freedom Act of 1998, 206
- Sales Tax and the Dormant Commerce Clause, 207
A New Sales Tax System: The Streamline Sales Tax Project (SSTP), 207
- Sales Tax Simplification Under the SSTP, 209
- Streamline Sales Tax Pilot: Sales Tax Compliance by an Outside Certified Service Provider (CSP), 211
- Internet Tax Moratorium and Equity Act, 211
International Internet Taxation, 211
- Organization of Economic Cooperation and Development Initiatives, 211
- National Initiatives Defining Permanent Establishment, 213
- European Union Value-Added Tax on Internet Sales, 214
Summary, 215
Key Terms, 215
Manager’s Checklist, 215
Case Problems, 216
Additional Readings, 218

8 Online Securities Offerings and Transactions, 219
Introduction, 219
Raising Capital: Online Securities Offerings, 220
Special Issues in Cyberspace

Privacy, 257

Introduction, 257
Sources of the Right to Privacy, 258
- U.S. Constitution, 258
- State Constitutions, 260
- Attorney-Client Privilege and the Use of E-Mail, 260
Common Law Torts for Invasion of Privacy, 260
- Intrusion upon Seclusion, 261
Katz v. United States, 261
- Privacy in the Use of Cellular Phones, 265
- Public Disclosure of Private Facts Causing Injury to Reputation, 265
- Publicity Placing Another in a False Light, 266
- Misappropriation of a Person's Name or Likeness Causing Injury to Reputation, 266

Federal Privacy Laws, 267
- Privacy Protection Act (PPA), 268
- Privacy Act of 1974, 268
- Cable Communications Protection Act (CCPA), 269
- Video Privacy Protection Act (VPPA), 270
- Telephone Consumer Protection Act (TCPA), 270

Federal Legislation: Credit and Financial Records, 270
- The Fair Credit Reporting Act (FCRA) of 1970, 270
- The Computer Fraud and Abuse Act (CFFA) of 1986, 271

Federal Legislation: Privacy in Personal Financial Information, 271
- Gramm-Leach-Bliley Act of 1999, 272
- Notice and Consent Requirements: Nonaffiliates, 273
- Identity Theft, 273
- Pretexting, 274

Federal Legislation: Privacy in Health and Medical Records, 274
- Health Insurance Portability and Accountability Act (HIPAA) of 1996, 274

Privacy Protection for Children from the Collection of Online Personal Information, 275
- The Children's Online Privacy Protection Act of 1998 (COPPA), 275
- COPPA: Safe Harbor, 276
- The Electronic Communications Privacy Act (ECPA) of 1986, 276
- Carnivore, 280

In Re DoubleClick Inc., Privacy Litigation, 281
- Title III: The Pen Register Act, 284

Privacy and Spam ("Unsolicited Commercial E-Mail"), 284
- Is Self-Regulation Working?, 286

Cyber Promotions, Inc., v. America Online, Inc., 288
CompuServe, Inc., v. Cyber Promotions, 290

Workplace Privacy, 292
- How Common Is the Problem of Employee Inappropriate Computer Use?, 293

Michael A. Smyth v. Pillsbury Company, 294
- Impact of the ECPA on Workplace Privacy, 297

Robert Konop v. Hawaiian Airlines, 297

Conclusion, 299

Global Issues of Privacy in Cyberspace, 301
- European Union Directive on Privacy Protection, 301
- The United States/European Union Safe Harbor Agreement, 302
- Other National Efforts at Regulating Internet Data Privacy, 304

Summary, 306
Immunity for Service Providers for Offensive Material, 349
Zeran v. America Online, Inc., 350
Sidney Blumenthal v. Matt Drudge and America Online, Inc. (AOL), 352
Anonymous Speech and Defamation, 356
SLAPP Suits, 357
International Regulation of Online Defamation, 358
- International Efforts to Regulate Cyber-Defamation, 358
- Internet Service Providers and International Acts of Defamation, 359
- Defamation and the International Choice of Law, 360
Ellis v. Time, 361
Summary, 362
Key Terms, 363
Manager's Checklist, 363
Case Problems, 364
Additional Readings, 366

12 Internet and Information Security, 367
Introduction, 367
The Challenges of Internet and Information Security, 368
The Goals of Internet and Information Security, 369
- Methods and Legal Challenges to Ensuring Enterprise and Communications Security, 371
- Transactional Security Systems, 372
- First Amendment, 377
- Regulating the Export of Cryptography Products, 381
Junger v. Daley, 382
Bernstein v. U.S. Department of Commerce, 384
- Judicial Opinion, 385
- Fourth Amendment, 385
Kyllo v. United States, 387
United States v. Scarfo, 392
- Fifth Amendment, 395
Karn v. Department of State, 395
International Aspects of Internet and Information Security, 397
- Global Network and Information Security, 397
- Encryption and Cryptography Systems, 398
Summary, 401
Key Terms, 401
Manager's Checklist, 402
Case Problems, 402
Additional Readings, 404
13 Internet and Computer Crime, 405

Introduction, 405
The Nature of Computer Crime, 406
- What Are Computer and Internet Crimes?, 407
- The Impact on Law Enforcement, 408
- The E-Commerce Risks, 410

The Role of Computers in Crime: Crimes and Perpetrators, 410
- How Computers Are Used in the Commission of Crimes, 410

Crimes Being Committed in Today's Networked Environment, 411
- Crimes Against Persons or Businesses, 412
United States v. Sample, 412
Ashcroft v. Free Speech Coalition, 417
- Crimes Against Property, 421
United States v. Morris, 422
United States v. Czubinski, 423
- Crimes Against Intellectual Property, 426
United States v. Rothberg, 427
- Other Federal Laws Invoked in Internet and Computer Crime Prosecutions, 431
- Crimes Against Government or Government Functions, 433

Corporate Forensics and the Impact of the Internet: Gathering and Preserving Evidence, 435
International Aspects of Internet Crime, 437
- Council of Europe Convention on Cybercrime, 438
- European Commission Communication on Computer-Related Crime, 439
- Successful International Cooperation Combating Cybercrime: The Bloomberg Example, 440

Summary, 441
Key Terms, 442
Manager's Checklist, 442
Case Problems, 443
Additional Readings, 444

Appendices, 445
Glossary, 505
Index, 513
Preface

“Clicks and bricks” is a vital business model in today’s competitive e-commerce environment. Managing in this milieu necessitates a basic understanding of cyberlaw as online business transactions develop at an exponential pace. Courts, legislatures, administrative agencies, and international directives all contribute to the e-commerce legal landscape of the 21st century. As digital technology continues to permeate every facet of business, the latest laws relevant to this phenomenon are explained and discussed in this second edition.

Since the first edition of CyberLaw: Text and Cases, we have witnessed the dot com demise, a languishing economy, an aggressive attitude by content providers to protect all of their intellectual property interests, a challenge to the U.S. Supreme Court on the duration of a copyright, an awareness of a loss of online privacy, and other dramatic new legal developments that we address in this second edition. The authors’ predominant concern continues to be producing a textbook that will be useful to instructors in preparing business students to manage in the high-tech legal environment. Because the potential liability exposure of a contemporary business is so vast, understanding the legal consequences of e-commerce transactions is not a luxury for the business manager. This textbook explains and discusses the “corpus juris” of cyberlaw from a business and social perspective. The values of the U.S. Constitution and ethical dilemmas are addressed throughout the textbook. Global issues as they relate to each chapter are explained as an essential component of the online environment.

The authors hope that instructors and students enjoy this business journey through cyberspace as each chapter reveals the legal consequences of transactions in the online environment. We are striving to educate managers to understand the legal, social, and ethical consequences of their business decisions.

Subject Matter and Basic Organization of the Text

The subjects covered follow a logical application of the legal issues surrounding e-commerce. The book’s focus is on the needs of business managers working, in some fashion, in the online environment. The authors are convinced that this includes the needs of almost every business school graduate about to enter the work force.

Accreditation

The subject matter of the textbook covers ethical, political, and international issues as well as a main focus on technology as it relates to the world of business. This makes a course in cyberlaw suitable for American Assembly of Collegiate Schools of Business (AACSB) accreditation.
OUTLINE OF THE TEXT

Part 1—Introduction to Cyberspace

Chapter 1—Technology and Cyberlaw. A revision of the chapter in the first edition, the authors discuss the technological infrastructure of the Internet and World Wide Web in the context of cyberlaw. The chapter offers a brief history of the Internet and outlines technologies such as firewalls, encryption, HTML, and cookies for nontechnical readers. The chapter broadens the focus on electronic commerce and updates the technology coverage to include filtering software and peer-to-peer technologies such as instant messaging and file sharing.

Chapter 2—Jurisdiction. Because e-commerce is global in nature, this chapter reviews the laws relevant to a court in a foreign state or country having personal jurisdiction over an e-business. This chapter reviews the laws relevant to a court’s personal jurisdiction over a nonresident e-business, including the principles of national enforcement that define a country’s power beyond its borders. The famous Yahoo!/France case is discussed along with Pavlovich, Verizon Online Services, and America Online.

Part 2—Intellectual Property Issues in Cyberspace

Chapter 3—Trademarks. Online liability exposure continues to focus on domain name arbitration and litigation. The laws of trademarks are explained with a discussion of the Anticybersquatting Consumer Protection Act, the Uniform Domain Name Dispute Resolution Policy, trademark infringement, and trademark dilution. Cases include a WIPO arbitration decision involving Julia Roberts and other cases such as Checkpoint Systems, A.B.C. Carpet Company, E&J Gallo Winery, and the leading meta-tag case of Playboy Enterprises v. Welles.

Chapter 4—Copyrights. The use of digital content in e-commerce continues to challenge conventional copyright laws regarding fair use. This chapter provides a general overview of copyright law as it applies to the online environment. The Digital Millennium Copyright Act is discussed along with leading cases, including the U.S. Supreme Court decision of Eldred v. Ashcroft on the duration of a copyright, and Napster and the Religious Technology Center cases.

Chapter 5—Business Methods Patents and Trade Secrets. An entirely new chapter, this material covers all aspects of managing these forms of intellectual property. We discuss legal and business strategies, as well as how to manage challenges relating to claims, inventorship, and infringement. Often overlooked as an alternative, we provide ample discussion of trade secrets, along with recent cases. These cases cover disputes involving: Amazon, Barnes & Noble, Pepsi, Priceline.com, State Street Bank & Trust Company, and Signature Financial Group.

Part 3—Business and Financial Issues in Cyberspace

Chapter 6—Online Contracting. A revision of the previous chapter, this material covers critical legal aspects of forming, performing, and enforcing online contracts.
This chapter examines the requirements for creating a contract, online warranties, and other terms of use provisions common in cyberspace. The Uniform Computer Information Transactions Act and the Uniform Electronic Transactions Act are also reviewed, with up-to-date commentary on interpretations of these important acts. After a discussion of electronic signatures and software licensing, the chapter discusses recent issues arising from shrinkwrap agreements, e-commerce insurance policies, and international matters.

Chapter 7—Sales Tax in E-Commerce. An e-business must consider the potential obligation of collecting sales tax on behalf of the state where it has a tax nexus. This chapter reviews the U.S. Constitution’s limitation on tax jurisdiction, the Internet Tax Freedom Act, sales tax and the dormant commerce clause, the latest development of the Streamline Sales Tax Project, along with the leading cases in this area, including National Bellas Hess and the leading U.S. Supreme Court case of Quill Corp. v. North Dakota.

Chapter 8—Online Securities Offerings and Transactions. A revision of the previous chapter, this material condenses coverage of the laws governing online offerings and expands coverage of online transactions. The chapter focuses on why capital is needed, where to find capital, and the offering process. We have selected entirely new cases, and we cover disputes involving such issues as selling stock in virtual companies, Internet offerings of nonexistent shares, investors suing after enormous price declines in the stock, and financial publishers duped into publishing false press releases in which share prices are consequently affected. The cases cover disputes involving SG, Ltd., Abacus International Holdings, Max Internet Communications, Internet Wire, and Bloomberg News.

Part 4—Special Issues in Cyberspace

Chapter 9—Privacy. This chapter has been revised and updated. It retains discussions of the sources of the right to privacy but expands the discussion of privileged communications under state law. Major emphasis is placed on recent federal legislation including the collection and use of personal information contained in medical (Gramm-Leach-Bliley Act of 1999) and financial records (Health Insurance Portability and Accountability Act of 1996). New materials are presented regarding children’s privacy, identity theft, pretexting, Carnivore—the FBI’s surveillance tool, and spam. TheDoubleClick case has been added to the discussion of the Electronic Communications Privacy Act (ECPA) as well as a new section regarding the Pen Register Act (Title III of the ECPA). Workplace privacy has been expanded to include new cases as well as suggestions for a computer usage and monitoring policy. The chapter concludes with a focus on the major global privacy issues with emphasis on the European Privacy Directive.

Chapter 10—Obscenity. The Internet allows the publication of pornography and obscene material. This chapter has updated discussions of the relevant cases and legislation regarding the ongoing, albeit ineffective, efforts of Congress to protect children from pornography and the issues posed to these efforts by the First Amendment. Two new cases are presented. U.S. v. Playboy Entertainment Group involves the issues
surrounding blocking children's access to adult cable programming, and *Ashcroft v. American Civil Liberties Union* involves the issue of whether or not community standards can be used to determine if material is obscene and therefore not suitable for children. The sections on employee access to adult Web sites and global obscenity issues have also been updated.

**Chapter 11—Defamation.** Cyberspace is a forum for defamatory speech. This chapter focuses on the major issues of defamation in cyberspace. There are revisions, updated discussions, cases, and materials related to the issues of jurisdiction and defamation, and the liability and immunity for service providers under the Communications Decency Act of 1996. A new section on anonymous speech has been added, including a discussion of the so-called *John Doe* cases in which a plaintiff in a suit for defamation attempts to obtain a subpoena to determine the identity of the alleged defamer. One such recent case is *Dendrite International, Inc. v. John Doe*. There is also a new section on SLAPP suits (Strategic Lawsuits Against Public Participants) in which corporations, government officials, and others attempt to use defamation suits against plaintiffs who express their opinions, criticisms, and comments online. The chapter concludes with revised discussions of the international issues of defamation. *Ellis v. Time, Inc.*, is presented to illustrate a case where a plaintiff attempted to convince a U.S. court to apply English libel law to allegedly defamatory statements and an e-mail message posted online in England.

**Chapter 12—Internet and Information Security.** A revision of the first edition chapter, we first discuss the purposes of information security and how this is achieved—a complex effort due to the open architecture of the Internet. Major emphasis is on transactional security systems, especially those involving cryptography. We outline the major challenges to the use of cryptography. Finally, we review government efforts to promote information security. Focus is on how these efforts—such as the USA Patriot Act, Carnivore/DCS-1000 and Magic Lantern/Key Logger Systems—impact our constitutional rights. There are five new cases in this chapter, and just one case from the first edition: *Corley, Junger, Bernstein, Scarfo, Kyllo*, and *Karn*.

**Chapter 13—Internet and Computer Crime.** A revision of the first edition chapter, we discuss the various crimes being perpetrated over the Internet and how the Internet's architecture and relatively lax security procedures produce the perfect environment for Internet crime. We cite those laws that address cybercrime. Emphasis is on the business environment as well as on government functions. Finally, we discuss cyberterrorism and the government response to it. There are three new cases, and two cases from the first edition: *Sample, Free Speech Coalition, Czubinski, Morris*, and *Rothberg*.

**FEATURES**

**Manager's Checklist.** Each chapter provides a Manager's Checklist that offers suggestions useful to business managers working in online environments in an effort to reduce their companies' liability exposure. Also included in this section are ethical
issues that relate to the chapter topic. These checklists help blend the practical with the necessary theoretical legal analysis found in the case decisions.

**Web sites.** Throughout the textbook Web sites are noted that apply to the subject matter. They can be used for additional reading, legal resources, and topics of interest. The majority of these sites are called out in “http://” boxes integrated throughout the text.

**End-of-chapter short cases.** Five cases are included at the end of each chapter for classroom testing or discussion of the material.

**Appendices.** Brief annotations from selected statutes relevant to the material covered in the text are found in the appendix at the end of the text. When available, we also provide the URL where the entire statute can be found.

**SUPPLEMENTS**

An **Instructor’s Manual**, prepared by the text authors, is available. For each chapter, the manual includes a chapter summary, a chapter outline, a suggested lecture outline, answers to the case questions, a suggested student assignment, and answers to the end-of-chapter case problems.

A **Test Bank**, prepared by John Hayward, Bentley College, is available to adopters. It includes approximately 35 to 40 multiple-choice questions and 2 to 3 short essay questions per chapter.

A set of **PowerPoint slides** designed to enhance lectures is available to adopters.

A **Text Web Site** at [http://ferrera.westbuslaw.com](http://ferrera.westbuslaw.com) is available for both instructors and students. It contains links to Web sites referenced in the text and case updates. Both students and instructors can download the PowerPoint slides from this Web site. Also, instructors can download the Instructor’s Manual and the Test Bank (both are also available in print form).

**Westlaw.** Ten complimentary hours of Westlaw are available to qualified adopters from West’s premier legal research system.

**West’s Video Library.** Qualified adopters may choose from West’s vast video library including Court TV® and Drama of the Law videos. For a complete listing of videos that are available, go to [http://www.westbuslaw.com](http://www.westbuslaw.com).

**ACKNOWLEDGMENTS**

We would like to thank the following reviewers of this book for taking time from their demanding schedules and providing their helpful suggestions:

Jason Ashford
Macon State College
Jeanne Calderon
New York University

Mark Conrad
Fordham University

Lori K. Harris-Ransom
Caldwell College

John C. Lautsch
California State University, Fullerton

Owen McWhorter, Jr.
Texas Tech University

Pamela Samuelson
University of California at Berkeley

Diana Walsh
New Jersey Institute of Technology

We are thankful for the excellent work and advice of the West/Thomson Learning publishing team—Rob Dewey, Steve Silverstein, Chris Hudson—and especially Jan Lamar, whose guidance and counsel have been most appreciated and invaluable.

The Bentley College authors wish to thank President Joseph Morone, and former vice president and dean of faculty, H. Lee Schlorff, for their continued support and enthusiasm for this project, and chancellor and former president of Bentley College, Gregory H. Adamian, for his support and encouragement over the years; Roseann Cotoní, administrative assistant of the Law Department, for her assistance; and graduate student assistants Maria Pere-Perez and Li Zhu for their work on the Bentley College CyberLaw Center that provides valuable links to material relevant to the chapters in this textbook. In particular, Gerald Ferrera would like to thank his graduate assistant Li Zhu for her research on portions of his manuscript.

The Boston College author, Margo E. K. Reder, wishes to recognize the entire faculty and staff at the Carroll School of Management for encouraging this project and for its Celebration of Scholarship. Particular thanks are due to Christine Neylon O’Brien, chair of the Business Law Department. She has cheered me on for fifteen years, and through her example, showed me how to excel—always with kindness and humor. Finally, I wish to thank Dave Twomey, past chair of the Business Law Department, for his interest in faculty development, and as an example to me in achieving high teaching standards.

Gerald R. Ferrera
Stephen D. Lichtenstein
Margo E. K. Reder
Robert C. Bird
William T. Schiano
### List of Cases

Note: The principal cases are in **bold** type. Cases cited or discussed in the text are in roman type.

<table>
<thead>
<tr>
<th>Case Title</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A&amp;M Records, Inc., et al. v. Napster, Inc.</td>
<td>103</td>
</tr>
<tr>
<td>A.B.C. Carpet Co., Inc., et al. v. Naeini</td>
<td>64</td>
</tr>
<tr>
<td>ACLU et al. v. Reno</td>
<td>327</td>
</tr>
<tr>
<td>ACTV, Inc. v. Walt Disney Co.</td>
<td>129</td>
</tr>
<tr>
<td>ALS Scan, Inc., v. Digital Services Consultants, Inc.</td>
<td>344</td>
</tr>
<tr>
<td>Am. Online, Inc. v. Superior Court (Mendoza)</td>
<td>33</td>
</tr>
<tr>
<td>Amazon.com, Inc. v. Barnesandnoble.com, Inc.</td>
<td>126</td>
</tr>
<tr>
<td>American Geophysical Union v. Texaco, Inc.</td>
<td>99</td>
</tr>
<tr>
<td>American Guarantee &amp; Liability Insurance Company v. Ingram Micro, Inc.</td>
<td>184</td>
</tr>
<tr>
<td>American Library Association (ALA) v. United States</td>
<td>331</td>
</tr>
<tr>
<td>Andersen Consulting, LLP v. UOP</td>
<td>277</td>
</tr>
<tr>
<td>Apple Computer v. Formula International</td>
<td>91</td>
</tr>
<tr>
<td>Ashcroft v. American Civil Liberties Union</td>
<td>328, 419</td>
</tr>
<tr>
<td>Ashcroft v. Free Speech Coalition</td>
<td>325, 417</td>
</tr>
<tr>
<td>AT&amp;T Corp. v. Excel Communications, Inc.</td>
<td>122</td>
</tr>
<tr>
<td>Bartnicki v. Vopper</td>
<td>265</td>
</tr>
<tr>
<td>Bensusan Restaurant Corp., v. King</td>
<td>31</td>
</tr>
<tr>
<td>Bernstein v. U.S. Department of Commerce</td>
<td>384</td>
</tr>
<tr>
<td>Blakey v. Continental Airlines</td>
<td>294</td>
</tr>
<tr>
<td>Bloomingdale’s v. Dept. of Revenue</td>
<td>206</td>
</tr>
<tr>
<td>Brower v. Gateway 2000, Inc.</td>
<td>179</td>
</tr>
<tr>
<td>Burger King Corp. v. Rudzewicz</td>
<td>21, 22, 33</td>
</tr>
<tr>
<td>Calder v. Jones</td>
<td>26</td>
</tr>
<tr>
<td>Carafano v. Metrosplash.com, Inc.</td>
<td>355</td>
</tr>
<tr>
<td>Carpenter v. United States</td>
<td>242</td>
</tr>
<tr>
<td>CCC Information Services, Inc., v. McAllen Hunter Market Reports, Inc.</td>
<td>93</td>
</tr>
<tr>
<td>Checkpoint Systems, Inc. v. Check Point Software Technologies, Inc.</td>
<td>59</td>
</tr>
<tr>
<td>Clapper v. Freeman Marine Equipment</td>
<td>151</td>
</tr>
<tr>
<td>Coastal Video Comm. Corp. v. Staywell Corp.</td>
<td>29</td>
</tr>
<tr>
<td>Columbia Pictures, Ind. v. Aveco, Inc.</td>
<td>94</td>
</tr>
<tr>
<td>Comb v. PayPal, Inc.</td>
<td>165</td>
</tr>
<tr>
<td>CompuServe, Inc., v. Patterson</td>
<td>29, 31</td>
</tr>
<tr>
<td><strong>CompuServe, Inc., v. Cyber Promotions</strong>, 288, 290</td>
<td></td>
</tr>
<tr>
<td>Cubby, Inc. v. CompuServe, Inc.</td>
<td>345</td>
</tr>
<tr>
<td>Curtis Publishing Co. v. Butts</td>
<td>348</td>
</tr>
<tr>
<td>Cyber Promotions Inc., v. America Online, Inc.</td>
<td>288</td>
</tr>
<tr>
<td>Dendrite International Inc., v. John Doe</td>
<td>357</td>
</tr>
<tr>
<td>Diamond v. Chakrabarty</td>
<td>115</td>
</tr>
<tr>
<td>Diamond v. Diehr</td>
<td>115, 118</td>
</tr>
</tbody>
</table>
DVD Copy Control Association v. Bunner, 138
E & J Gallo Winery v. Spider Webs Ltd., 68
Eldred v. Ashcroft, 88, 89, 113
Ellis v. Time, 361
Encyclopedia Britannica Ed. Corp. v. Crooks, 98
Erienet, Inc., et al., v. Velocity Net, Inc., et al., 270
FCC v. Pacifica Foundation, 321
Feist Publications, Inc. v. Rural Telephone Services Inc., 93
Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co., Ltd., 129
Free Speech Coalition v. Reno, 325
FTC v. GM Funding, Inc., Global Mortgage et al., 286
FTC v. Toysmart.com, 275
Gertz v. Robert Welch, 347
Griswold v. Connecticut, 259
Gutnick v. Dow Jones, 359
Haack v. Max Communications, Inc., 228
Hart v. Internet Wire & Bloomberg L.P., 237
Hasbro, Inc. v. The Internet Entertainment Group, 66
Helikopteros Nacionales de Colombia, S.A. v. Hall, 28
Hilton v. Guyot, 362
Immunomedics, Inc. v. Doc, 357
In re Alappat, 115
In re DoubleClick Inc., 258, 281
In the Matter of Eli Lilly, 267
Ingenix, Inc. v. Lagalante, 140
Int'l Federation of the Photographic Industry v. Olsson, 105
International Shoe Company v. Washington State, 24, 25
Julia Fiona Roberts v. Russell Boyd, 54
Junger v. Daley, 382
Karn v. Department of State, 395
Katz v. U.S., 261, 276, 386
Kyllo v. United States, 258, 387
La Salle Nat’Bank v. Viro, 28
Lewis Galoob Toys, Inc. v. Nintendo, Inc., 93
Lockheed Martin Corp. v. Network Solutions, Inc., 53
Lunney v. Prodigy, 348
M.C.B. Homes, Inc. v. Ameron Homes Inc., 85
MAI Systems Corp. v. Peak Computer, Inc., 91
Marcus v. Rowley, 98
Marketel International Inc. v. Priceline.com, 123
Marobie-Fl. Inc. v. National Ass’n of Fire Equip. Distrbs., 92
McDonald v. Paton, 358
McFarlane v. Sheridan Square Press, 361
McIntyre v. Ohio Elections Commission, 356
McLaren v. Microsoft, 296
McVeigh v. Cohen et al., 278
Memoirs v. Massachusetts, 314
Michael A. Smyth v. Pillsbury Company, 294
Michaels v. Internet Entert. Group, Inc., 94
Millennium Enterprises, Inc., v. Millennium Music, et al., 22, 42
Miller v. California, 313, 315
Motion Picture Arts and Sciences v. Network Solutions, Inc., 53
Nardinelli et al. v. Chevron, 293
National Bellas Hess, Inc. v. Dept. of Rev. of the State of Illinois, 197, 198
Netscape Communications Corp. v. Microsoft Corp., 130
New Energy Co., of Ind. v. Limbach, 207
New York v. Ferber, 331
O’Connor v. Ortega, 292
Osborne v. Ohio, 332
Paris Adult Theatre I v. Slaton, 319
Pavlovich v. The Superior Court of Santa Clara County and DVD Copy Control Assn., Inc., 26
Pennoyer v. Neff, 23
PepsiCo, Inc. v. Redmond, 138
Playboy Enter. Inc., v. Frena, 92, 94
Playboy Enterprises Inc. v. Welles, 73
Playboy Enterprises v. Calvin Designer Label, 79
Pope v. Illinois, 318
ProCD, Inc. v. Zeidenberg, 177
Quill Corp. v. North Dakota, 193, 201, 211
Recording Industry Association of America (RIAA) v. Verizon Internet Services, 356
Religious Technology Center v. Netcom On-Line Communication Services, Inc., 95
Reno v. American Civil Liberties Union (Reno 1), 321
Restuccia v. Burk Technology, 297
Reves v. Ernst & Young, 221
Robert Konop v. Hawaiian Airlines, 297
Rosenblatt v. Baer, 347
Roth v. United States, 312
Sanders v. Robert Bosch Corp., 293
Santa Fe Natural Tobacco, Inc. v. Spitzer, 207
Securities and Exchange Commission v. Abacus International Holdings Corp., 226
Securities and Exchange Commission v. Gold-Ventures Club, 244
Securities and Exchange Commission v. SG Ltd., 222
Securities and Exchange Commission v. W. J. Howey Co., 221
Securities and Exchange Commission v. Zandford, 224
Sega Enterprises Ltd. v. MAPHIA, 95, 281
Sidney Blumenthal v. Matt Drudge and America Online, Inc. (AOL), 352
Smith v. California, 348
Sony Corp. v. Universal Studios, Inc., 86, 98
Specht v. Netscape Communications Corp., 179
Stanley v. Georgia, 319
Stanley Young v. The New Haven Advocate, et al., 344
State Auto Property & Casualty Insurance Company v. Midwest Computers & More, 183
State of Washington v. Heckel, 284
State Street Bank and Trust Co. v. Signature Financial Group, Inc., 115, 119, 120, 122, 130
Steele v. Bulova Watch Co., 106
Stern v. Delphi Services Corporation, 266
Stratton Oakmont, Inc. v. PRODIGY Services Company, 349
Subafilms, Ltd v. MGM-Pathe Communications, 106
The Bremen v. Zapata Off-Shore Co., 33
The Petition for Redetermination of Barnes & Noble.com, 206
Toys R Us, et al. v. Richard Feinburg, 67
Toys R Us v. Akkaoui, 67
TRW, Inc. v. Andrews, 415
Two Pesos, Inc. v. Taco Cabana, Inc., 50
Tyler Pipe Industries, Inc. v. Dept. of Revenue, 206
U.S. v. Acheson, 325
U.S. v. American Library Association, 331
U.S. v. Hilton, 325
U.S. v. Playboy Entertainment Group, Inc., 322
U.S. v. Slanina, 334
U.S. v. Thomas, 316
United States v. Baker, 421
United States v. Czubinski, 423, 432
United States v. Hunter, 436
United States v. Morris, 422
United States v. Mullins, 278
United States v. Petersen, 408
United States v. Rothberg, 427
United States v. Sample, 412
United States v. Scarfo, 392
United States v. Thomas, 416
Universal Studios, Inc. v. Corley, 38, 102, 118
Urosky et al. v. Gilmore, 334
Vanity Fair Mills, Inc. v. T. Eaton Co., 107
Verizon Online Services, Inc. v. Ralsky, 29
Wal-Mart Stores, Inc. v. Samara Brothers, Inc., 50
Wang Meng v. Century Internet Communications Technology Co., 105
Washington Speakers Bureau, Inc. v. Leading Authorities, Inc., 64
Watkins v. L.M. Berry and Co., 293
Weld v. CVS Pharmacy, Inc., et al., 267
Wilson v. Black-bird Creek Marsh Co., 207
Winans v. Denmead, 128
World Wide Volkswagen Corp. v. Woodson, 21, 25
Yahoo!, Inc. v. La Ligue Contre Le Rascime et L’Antisemitisme, 37
Zeran v. America Online, Inc., 350
Zeran v. Diamond Broadcasting, Inc., 352
COPYRIGHTS

Napster harms the market in "at least" two ways: it reduces audio CD sales among college students and it raises barriers to plaintiffs' entry into the market for the digital downloading of music.


LEARNING OBJECTIVES

After you have read this chapter you should be able to:

1. Explain what subject matter may be copyrighted on an e-business Web site.
2. Explain and discuss the exclusive statutory rights granted to the online owner of a federally registered copyright.
3. Explain the statutory limitations on the exclusive statutory rights of an online copyright owner.
4. Understand the elements that make up the defense of "fair use" in the online context.
5. Explain the duration of copyright protection.
6. Explain and understand the difference between direct, contributory, and vicarious infringement.
7. Explain copyright liability to online service providers.
8. Understand the significance of the Digital Millennium Copyright Act.
9. Explain the legal remedies for a copyright infringement.
10. Understand the various international copyright treaties.
11. Explain the factors involved in determining when an international copyright can be enforced in a U.S. court.

INTRODUCTION

Napster, discussed later in this chapter, would be a thriving business today were it not for copyright law. This chapter will help you understand the copyright issues relevant to an e-business and assist you in reviewing e-commerce from a copyright law perspective.
An e-business has two major concerns regarding copyright law: first, to protect its Web site from potential infringers who may copy parts or all of their content without permission, and second, to be sure its Web pages are not infringing on another owner's copyrighted material. Furthermore, your Web site may link to another site that displays copyrighted material without the owner's consent. Could your e-business be sued under a theory of copyright infringement? Is there a legal strategy to be utilized that may limit this potential liability exposure? This chapter discusses these and other issues relevant to copyright protection and liability.

Digital content, transmitted over the Internet, creates unique copyright issues. Web page words, videos, music, Terms of Use and privacy policies, providing they are "original works," may be the appropriate subject matter of copyright protection and federal registration in the U.S. Copyright Office. Copyright law does not protect ideas, systems, or business methods. For example, copyright law does not protect your ideas and graphs expressed in an original business plan, but the original written and graphic description is protected. In addition to copyright law, you should exercise your trade secret rights in your business plan (discussed in Chapter 5).

Federal copyright law provides the owner of an original work of authorship with exclusive statutory rights, discussed in this chapter. Because Web site design and development are costly ventures, legally protecting them with copyright ownership incurs a special significance on the Internet. Furthermore, the improper use of e-mail may implicate copyright liability. For example, an e-mail user may send, without the owner's permission, an attached copy of a copyrighted document that is reproduced in perfect form to a vast global audience. This inappropriate use of electronic communication poses special and unique problems for copyright protection on the Internet.

As previously stated in Chapter 3, "Trademarks," copyright law has historically been a form of intellectual property along with trademarks, patents, and trade secrets. Trademarks, not copyrights, legally protect business names, advertising slogans, and short phrases used to distinguish goods and/or services sold in interstate commerce. Patents, not copyrights, may protect business methods, discussed in Chapter 5, "Business Methods Patents and Trade Secrets." Copyright legally protects a vast array of "original works of authorship fixed in a tangible medium of expression" including:

- computer software and architecture (code)
- movies and other audiovisual works, including those on a Web site
- musical compositions, including the lyrics of the song
- novels, including e-books
- poetry
- literary works, including Web site content
- dramatic works
- sound recordings, including Web site audio transmissions
- pantomimes and choreographic works
• sculptural works
• architectural works

The origin of U.S. copyright law is found in the first English copyright act, the 1710 Statute of Anne. Although the common law provides the author of "original and creative works" with copyright protection as soon as it is "fixed in a tangible form," filing the work for registration in the U.S. Copyright Office is a prerequisite for initiating a legal claim for copyright infringement in the federal court system [M.C.B. Homes, Inc. v. Ameron Homes Inc., 903 F.2d 1486, 1488 (11th Cir. 1990)].

Copyright law is federal law found in the Copyright Act [17 U.S.C. 101-1205] that protects the authors from copyright infringement for "original works of authorship fixed in a tangible medium of expression" [17 U.S.C. Sec. 401 (d)]. Because the original content on Web pages qualifies for federal registration of the site in the U.S. Copyright Office, one of the first orders of business of an e-business should be to file for federal copyright registration of its Web pages.

Providing the entire content of the Web pages are "original works of authorship," the online venture satisfies the statutory requirement that it be "fixed in a tangible medium of expression." Web site developers must be especially aware of copyright issues that may have legal consequences at a later time when a great deal of effort and cost have been expended to create or update an e-company’s Web site.

Because designing, producing, and maintaining a sophisticated Web site is very expensive, protecting content ownership is extremely important. Electronic commerce will continue to be highly competitive. As Web sites become more and more interactive with consumers, their creation, design, and maintenance place enormous demands on innovative marketing techniques that should be legally protected.

Framers of the U.S. Constitution knew the value of protecting exclusive rights in the owner of creative works. The authority of Congress to enact copyright laws is found in Article I, Section 8, clause 8: The Constitution grants power in Congress "to promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries." This exclusive property interest gives the copyright owner of a Web site a monopoly in the work. However, the free flow of information that is the very culture and value of the World Wide Web may conflict with this copyright interest. The First Amendment's history of freedom of speech encourages the currency of ideas and their expression, no matter how controversial. Creative information and, indeed, commerce itself, depends on the development of commercial expression. Balancing these competing interests is the purpose of the U.S. Copyright Act and the federal courts.

Keep in mind that never before has it been so easy to violate a copyright owner's exclusive right to copy the material. Common copyright violations are employees

Visit the federal Copyright Office Web site to see detailed information on copyright law:
http://lcweb.loc.gov/copyright
forwarding or attaching copyrighted e-mail without the consent of the author. Both methods may violate the owner’s exclusive statutory right to copy the document.

The uploading of information and making multiple copies of online material could also be a copyright violation, as well as the downloading of MP3 files (http://www.mp3.com). Companies and individuals that are not aware of these copyright infringements may find themselves liable under legal theories discussed later.

Copyright law is a strict liability statute. This means it is possible to be liable as an unintentional infringer, and hence the importance of an e-business working closely with its lawyers cannot be overestimated. This chapter reviews the copyright laws of e-commerce and acquaints you with some of the copyright problems relative to the online environment. Suggestions are made throughout the chapter as to how an e-business manager can legally protect copyright ownership and limit a company’s copyright liability (see Figure 4.1).

**Copyright Act of 1976**

In order to implement the congressional authority as stated in the U.S. Constitution of granting exclusive rights to copyright owners, Congress adopted in 1790 the first U.S. copyright law. The statute has gone through numerous amendments, resulting in a comprehensive revision in 1909. As our mass media evolved from radio to movies to VCRs, to audio and videotapes, Congress again saw fit to amend the Copyright Act in 1976. The act took effect on January 1, 1978.

The federal courts’ function is to interpret the Copyright Act within the context of our current environment of information technology. As stated by the U.S. Supreme Court, “From the beginning, the law of copyrights has developed in response to significant changes in technology” [Sony Corp. v. Universal Studios, Inc., 464 U.S. 417 (1984)]. The role of the court, however, remains constant. It must maintain the del-

---

**FIGURE 4.1 E-Business Copyright Objective and Legal Strategy**

**E-business objective:** Protect the Web pages of the company’s Web site from being copied by other companies and protect the company from any copyright infringement suits.

**Legal strategy:**

- Register the copyright of the Web pages.
- Include appropriate disclaimers in the Terms of Use for copyright infringement by linked companies.
- Monitor bulletin boards and chat rooms for known copyright infringements by third parties.
icate balance between the exclusive rights of copyright owners and the public's right to have access to information (discussed later under the "fair use" doctrine).

**Subject Matter of Copyrights**

Copyright ownership can be registered for (1) literary works, (2) musical works, (3) dramatic works, (4) pantomimes/choreographic works, (5) pictorial, graphic, and sculptural works, (6) motion pictures and audiovisual works, (7) sound recordings, and (8) architectural works.

In order for this material to be registered in the Copyright Office as a copyright, it must be "an original work of authorship fixed in any tangible medium of expression from which they can be perceived, reproduced, or otherwise communicated either directly or with the aid of a machine or devise" [17 U.S.C. Sec. 102 (a)]. This requirement may fit the application of the material found on Web pages, allowing them to be federally registered with the U.S. Copyright Office (see Figure 4.2).

The nature of its originality requires the work be a creative document not copied from another source. It must be the independent work of the author. Under the Copyright Act, a **fixed creative work** is fixed "when its embodiment in a copy or phonorecord . . . is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration" (17 U.S.C. Sec. 101). Fixed creative works must be fixed in a tangible medium of expression in order to be copyrighted. Web pages fit this statutory requirement and may be federally registered. The Copyright Act clearly states that an original work of authorship does not extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, unless fixed in a tangible form [17 U.S.C. Sec. 102(b)]. Copyright law protects the expression of an idea and not the idea itself.

Although you cannot copyright a creative and original idea, once the idea is expressed in a fixed, tangible form, it may acquire copyright protection. For example, the contents on a Web page were once original and creative ideas, but when coded and fixed in floppy disks, compact disks, or other digital storage devices, printed copies of this material may be sent with the application to the Copyright Office for federal copyright registration. Notice that a system or method of operation is not a subject matter for a copyright. However, an appropriate "business method" may be patentable. (See Chapter 5, "Business Methods Patents and Trade Secrets.")

**FIGURE 4.2 Criteria for Copyright Protection of a Web Page**

- **Originality**—The Web site may not copy a similar site and should strive for a unique presentation (e.g., http://www.consumerreview.com).
- **Creativity**—The Web site need not be novel, as in a patent requirement, but should be an independent creation (e.g., http://www.landsend.com).
- **Fixed form**—The application of the content to the Web site is sufficient to create a fixed form for copyright protection purposes.
Original and creative digital works fixed in a tangible medium of expression will receive exclusive statutory rights under copyright law. This is the basis for Web site federal registration in the U.S. Copyright Office.

Requirements for Registration in the Copyright Office

Registration of a copyright in the Copyright Office requires a completed registration form and a submission of the original work. The Copyright Office will then issue to the owner a certificate of registration. In a copyright infringement case, the plaintiff will submit this certificate to prove copyright registration and ownership. The certificate of registration constitutes prima facie evidence of the validity of the copyright and allows the owner to sue an infringer in the federal court and pursue statutory remedies. So the importance of federal registration of the e-business Web site cannot be overestimated. It provides the e-business with a property interest in the Web site that is legally protected.

Duration of Copyright

In October 1998, Congress enacted the Sonny Bono Copyright Term Extension Act (CTEA). It extends the term of most copyrights by twenty years. These changes harmonize U.S. law with European copyright laws.

Thus copyrights for works created prior to January 1, 1978, generally endure for a term of 28 years with the option to renew for a further term of 67 years. Prior to the CTEA, the renewal term was for 47 years [17 U.S.C. sec. 304].

Copyrights for works created on or after January 1, 1978, generally endure for a term consisting of the life of the author plus an additional 70 years after the author’s death. Prior to the CTEA the term after death was for 50 years [17 U.S.C. sec. 302].

Constitutional Challenge to the Sonny Bono Copyright Term Extension Act

The U.S. Supreme Court heard the case of Eldred v. Ashcroft, on the issue of whether or not the constitutional limits of congressional power to extend the term of copyright for twenty years has been exceeded as provided in the Copyright Clause that states, “Congress has the authority to issue copyrights ‘for limited times’ in order to ‘promote the progress of science and useful arts.’” The plaintiffs argued that copyright protection is a legal monopoly giving exclusive rights to the copyright owner, with some limitations for fair use, during the copyright duration. The traditional basis for that entitlement was to give the authors an incentive to write and publish material and at the same time to promote the progress of the arts. Petitioners argued that at some point this copyright protection should end and the copyrighted material should fall into the realm of public domain. They further argued to assure a vast public domain of free works is available for the common good, the retroactive extension for twenty years granted in the Sonny Bono Copyright Term Extension Act of 1998 was an abuse of congressional authority. As you read the case, note how the U.S. Supreme
Court responded to the objection that the copyright extension has an adverse effect on the public domain’s reception of expired copyrighted works and the right of Congress to grant a monopoly to copyright owners is subject to the limited time provision of the U.S. Constitution.

Eldred v. Ashcroft
123 S. Ct. 769

Facts

This case concerns the authority the Constitution assigns to Congress to prescribe the duration of Copyrights. The Copyright and Patent Clause of the Constitution, Art. I, Sec. 8, cl. 8, provides as to copyrights: “Congress shall have Power ... [t]o promote the Progress of Science ... by securing [to Authors] for limited Times ... the exclusive Right to their ... Writings.” In 1998, in the measure here under inspection, Congress enlarged the duration of copyrights by twenty years [Copyright Term Extension Act (CTEA), Pub. L. 105-298, Sec. 102(b) and (d), 112 Stat. 2827-2828 (amending 17 U.S.C. Sections 302, 304)]. As in the case of prior extensions, principally in 1831, 1909, and 1976, Congress provided for application of the enlarged terms to existing and future copyrights alike.

Petitioners are individuals and businesses whose products or services build on copyrighted works that have gone into the public domain. They seek a determination that the CTEA fails constitutional review under both the Copyright Clause’s “limited times” prescription and the First Amendment’s free speech guarantee.

In accord with the District Court and the Court of Appeals, we reject petitioners’ challenges to the CTEA. In that 1998 legislation, as in all previous copyright term extensions, Congress placed existing and future copyrights in parity. In prescribing that alignment, we hold, Congress acted within its authority and did not transgress constitutional limitations.

Petitioners’ suit challenges the CTEA’s constitutionality under both the Copyright Clause and the First Amendment.

We granted certiorari to address two questions: whether the CTEA’s extension of existing copyrights exceeds Congress’ power under the Copyright Clause; and whether the CTEA’s extension of existing and future copyrights violates the First Amendment. We now answer those two questions in the negative and affirm.

Judicial Opinion (Justice Ginsburg)

We address first the determination of the courts below that Congress has authority under the Copyright Clause to extend the terms of existing copyrights. Text, history, and precedent, we conclude, confirm that the Copyright Clause empowers Congress to prescribe “limited Times” for copyright protection and to secure the same level and duration of protection for all copyright holders, present and future.

To comprehend the scope of Congress’ power under the Copyright Clause, “a page of history is worth a volume of logic.” New York Trust Co. v. Eisner, 256 U.S. 345, 349
History reveals an unbroken congressional practice of granting to authors of works with existing copyrights the benefit of term extensions so that all under copyright protection will be governed evenhandedly under the same regime.

Congress' consistent historical practice of applying newly enacted copyright terms to future and existing copyrights reflects a judgment stated concisely by Representative Huntington at the time of the 1831 Act; "[J]ustice, policy and equity alike forbid" that an "author who had sold his [work] a week ago, be placed in a worse situation than the author who should sell his work the day after the passing of [the] act." 7 Cong. Deb. 424 (1831). The CTEA follows this historical practice by keeping the duration provisions of the 1976 Act largely in place and simply adding 20 years to each of them. Guided by text, history, and precedent, we cannot agree with petitioners' submission that extending the duration of existing copyrights is categorically beyond Congress' authority under the Copyright Clause.

Satisfied that the CTEA complies with the "limited Times" prescription, we turn now to whether it is a rational exercise of the legislative authority conferred by the Copyright Clause. On that point, we defer substantially to Congress. Sony, 464 U.S., at 429 stated ("[I]t is Congress that has been assigned the task of defining the scope of the limited monopoly that should be granted to authors . . . in order to give the public appropriate access to their work product.")

The CTEA reflects judgments of a kind Congress typically makes, judgments we cannot dismiss as outside the Legislature's domain.

The CTEA may also provide greater incentive for American and other authors to create and disseminate their work in the United States. "M]atching th[e] level of [copyright] protection in the United States [to that] in the EU can ensure stronger protection for U.S. works abroad and avoid competitive disadvantages vis-à-vis foreign rightholders."

In addition to international concerns, Congress passed the CTEA in light of demographic, economic, and technological changes.

In sum, we find that the CTEA is a rational enactment; we are not at liberty to second-guess congressional determinations and policy judgments of this order, however debatable or arguably unwise they may be. Accordingly, we cannot conclude that the CTEA—which continues the unbroken congressional practice of treating future and existing copyrights in parity for term extension purposes—is an impermissible exercise of Congress’ power under the Copyright Clause.

Petitioners separately argue that the CTEA is a content-neutral regulation of speech that fails heightened judicial review under the First Amendment. We reject petitioners' plea for imposition of uncommonly strict scrutiny on a copyright scheme that incorporates its own speech-protective purposes and safeguards. The Copyright Clause and First Amendment were adopted close in time. This proximity indicates that, in the Framers' view, copyright's limited monopolies are compatible with free speech principles. Indeed, Copyright's purpose is to promote the creation and publication of free expression. "[T]he Framers intended copyright itself to be the engine of free expression. By establishing a marketable right to the use of one's expression, copyright supplies the economic incentive to create and disseminate ideas." As we read the Framers' instruction, the Copyright Clause empowers Congress to determine the intellectual property regimes that, overall, in that
body’s judgment will serve the ends of the Clause. The wisdom of Congress’ action, however, is not within our province to second guess. Satisfied that the legislation before us remains inside the domain the Constitution assigns to the First Branch, we affirm the judgment of the Court of Appeals.

Case Questions

1. What were the petitioners’ grounds for this appeal?
2. What is the relationship of this case to the copyright law of the European Union?
3. Why did the court hold that the extended copyright duration for an additional twenty years did not violate the First Amendment’s free speech guarantee?

Exclusive Statutory Rights of a Copyright Owner

E-business owners of a federally registered copyright work have the following exclusive statutory rights that collectively define the scope of the copyright:

- To reproduce the copyrighted work
- To sell, rent, lease, or otherwise distribute copies of the copyright work to the public
- To prepare derivative works based on the copyright work
- To perform and display publicly the copyright work

Right to Reproduce the Work

Copyright infringement in the online environment often involves a violation of the reproduction right that occurs by transferring data from one computer to another. An early 1984 case, Apple Computer v. Formula International, 594 F. Supp. 617, held that copies stored in random access memory (RAM) were temporary, and running a computer program from RAM does not create an infringed copy.

However, in a 1993 case, MAI Systems Corp. v. Peak Computer, Inc. 1991 F.2d 511 (9th Cir. 1993), software was downloaded into RAM when the defendant turned the computer on in the course of performing maintenance. In doing so, the defendant was able to view the software program to assist him in diagnosing the problem. The court found that the copy created in RAM was sufficiently permanent and “fixed” to satisfy the Copyright Act and cause an infringement of the software. This case should alert the e-business manager that an unauthorized downloading of software onto RAM and using it for personal gain constitute both a “copying” and infringement.

Other instances of an unauthorized reproduction and copyright infringement are “scanning” a copyrighted printed document into a digital file and uploading and/or downloading a digital copyrighted file to a bulletin board system.
Right of Distribution: Selling, Renting, or Leasing Copies

Because a copyright is the exclusive property of the owner, the right to exercise property interests, such as selling, renting, or leasing the copyright, is protected by the court. A person who does not own the copyright and makes it available on a bulletin board service can be liable for copyright infringement.

In *Playboy Enter. Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993), the court held that when unauthorized photographs of Playboy Enterprises were downloaded to a bulletin board system by the defendant's subscribers, the plaintiff's exclusive right of distribution was infringed by customers of the defendant. Notice how a bulletin board operator, as the defendant in this case, has an obligation to monitor its system to ensure that copyrighted documents are not being displayed and "downloaded" by its customers.

The same rationale regarding the copyright owner's exclusive right of distribution applies to e-mail attached or forwarded without the permission of the copyright owner. This has become common company practice, and managers should be aware of the potential employer's copyright infringement liability.

In a 1997 case, *Marobie-Fl. Inc. v. National Ass'n of Fire Equip. Dists.*, 983 F. Supp. 1167 (N.D. Ill.), unauthorized copies of the plaintiff's electronic clip art files were placed on the defendant's Web page. The court held that this constituted an infringing distribution because the files were available for downloading by Internet users. Because this has become a common practice, Web designers as well as managers should be careful in obtaining permission from the owner of clip art if they want to use it on their Web sites.

**Linking to a Web Site.** Linking to a *surface page* (i.e., a home page that often displays the Web site's trademark, copyright, and "banner ads") by listing its URL (universal resource locator) is similar to giving directions to the listed site and is not a "copying" within the Copyright Act. Hence a surface link to a home page does not generally require permission. This position is based on the theory that going online creates an implied license for anyone with a computer to view the Web site.

However, the terms of use published in many sites restrict the user to making only one copy for personal use of any information displayed. This interactive feature of the WWW to hyperlink defines its very culture, distinguishing it from any other communications medium. E-business Web sites often link to other sites that provide the user with merchandise, helpful information, or resources related to the product and/or service being offered. It would be a prudent business practice to obtain permission to link. Entering into a Web-linking agreement with the linked site will avoid any misunderstanding regarding a copyright infringement.

Creators of a Web site who wanted assurance it was not linked to a pornographic or shabby site could place a prohibition in its Terms of Use similar to, "Do not link to this site without our express consent." This could negate any implied license to link by merely going online.

http://www.mapquest.com
Databases. Databases may be subject to copyright registration if the author is creative in selecting and arranging the data and does not merely display the data as facts. In a copyright infringement suit before the U.S. Supreme Court, defendant was the publisher of a telephone directory that reproduced over one thousand of the plaintiff's telephone numbers without its consent. The court found for the defendant and held that the plaintiff's mere arrangement of facts lacked originality because "there is nothing remotely creative about arranging names alphabetically . . . " [Feist Publications, Inc. v. Rural Telephone Services Inc., 499 U.S. 340 (1991)]. Note that the court denied copyright protection on the basis that the mere alphabetical listing of names and telephone numbers lacked originality.

A federal court in deciding an online case involving the "Red Book" that listed the retail value of used automobiles held the book would be granted copyright protection. The listings in the defendant's "Red Book" were found to be original because the compilation included the selection of optional features in a unique fashion, made an adjustment for mileage in 5,000-mile increments, and used the concept of an "average" vehicle as the subject of evaluation [CCC Information Services, Inc., v. McAllen Hunter Market Reports, Inc., 44 F.3d. 612nd Cir. 1994]).

This case is especially important in the online environment because information acquired from consumers is often compiled in a database, and in some instances it is sold to other merchants. (See Chapter 9, "Privacy.") To acquire copyright protection for the consumer database, it must be an original coordination and arrangement of the data. You could accomplish this by dividing the information into regional areas based on customer preference, and so on. Managers should be careful of being in compliance with the privacy policy posted on the company's Web site that makes representations to the users how the information will be used.

Right to Prepare Derivative Works

Web designers often examine various Web sites and select their most attractive features. The designers must be careful not to infringe on the copyright of another site by preparing a derivative work based on the original presentation.

The Copyright Act defines derivative work as "a work based upon one or more preexisting works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which a work may be recast, transformed or adopted" (17 U.S.C. sec. 101). A derivative work includes "a work consisting of editorial revisions, annotations, elaborations, or other modifications, which, as a whole, represent an original work of authorship . . . (17 U.S.C. sec. 101).

A federal court held that a "Game Genie" device that altered features in Nintendo's videogame cartridges did not create a derivative work. The "Game Genie" enhanced the audiovisual displays without incorporating the underlying work in any permanent form [Lewis Galoob Toys, Inc. v. Nintendo, Inc., 964 F.2d. 965 (9th Cir. 1992)].
To avoid a possible copyright infringement suit based on it being a derivative work, the Web site should not be an adaptation of another site. Managers should consider an indemnity contract with the Web site designer that will repay them for any loss sustained from this potential liability.

**Right to Perform and Display Publicly a Copyright Work**

The Copyright Act defines as public performance the performance that occurs at a place open to the public. It also includes a semipublic place or any place where a substantial number of persons outside of a normal circle of a family and its social acquaintances are gathered (17 U.S.C. Sec. 101).

In *Columbia Pictures, Ind. v. Aveco, Inc.*, 800 F.2d 59 (3rd. Cir. 1986), the defendant improperly authorized public performances by renting videotapes and allowed customers to see the tapes in viewing rooms. The court held that this constituted "a place open to the public" within the meaning of Sec. 101, on the theory that the rooms were open for "any member of the public to avail themselves of this service." Business managers who display Web material on a computer monitor in employee training programs, without the consent of the owner, may be opening this to the public. Within the statutory definition of a public place, you should obtain permission from the owner before doing so. Courts have held that making available videotape over the Internet without authorization and posting unauthorized copies of electronic clip art on Web pages could violate the copyright owner's exclusive statutory right of public display [*Michaels v. Internet Entert. Group, Inc.*, 5 F. Supp. 2d 823 (C.D. Cal. 1998)].

**Theories of Liability for Copyright Infringement**

There are three theories of copyright infringement liability: direct, contributory, and vicarious.

**Direct Infringement**

The direct infringer is the direct actor who, with or without a specific intent to infringe, is the primary party that violates one of the copyright owner's exclusive statutory rights. This is the person or company that actually carries out the direct infringement. The Copyright Act is a strict liability statute, meaning that knowledge or intent of infringement need not be proved by the plaintiff.

Bulletin board operators may be liable for the unauthorized distribution and display of images uploaded to and downloaded from their systems. A Florida court held that it was irrelevant the bulletin board system operator did not make the copies itself and thus found it liable for direct infringement [*Playboy Enters., Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993)].

A California court took a more realistic position and held there was no direct infringement of the statutory exclusive rights under the Copyright Act when the infringement was initiated by a third party. In now-famous legal language, the court stated, "although copyright is a strict liability statute, there should still be some element of volition or
causation which is lacking where a defendant’s system is merely used to create a copy by a third party.” The court reasoned that it would be inappropriate to apply direct infringement liability to a party such as an Internet service provider that acts like a conduit of information [Religious Tech. Ctr. v. Netcom On-Line Communications Services, Inc., 907 F. Supp. 1361 (N.D. Cal. 1995), discussed in full later in this chapter].

**Contributory Infringement**

**Contributory infringement** is the tort (civil wrong not based on contract) of contributing to the direct infringement of another. Although not mentioned in the Copyright Act, the legal theory developed by court decisions supporting contributory infringement liability is based on the fact that a person with knowledge or reason to know of the infringing activity causes or materially contributes to the conduct of the direct infringer. For there to be a contributory infringement claim there must first be a direct infringement by another person.

In *Sega Enterprises Ltd. v. Maphia*, the court did not find direct copyright infringement by the operator of an electronic bulletin board service but, nevertheless, found him liable for contributory infringement. The users of the bulletin board service were the direct infringers. The *Sega Enterprises Ltd. v. Maphia* case is one of the leading cases on contributory infringement. If a person has knowledge that a user is copying a document or could monitor such activity and carelessly avoided doing so, there is contributory copyright infringement. E-business managers must be aware of direct infringing taking place by their subordinates. For example, a company could be liable for contributory infringement if a manager knows an employee is consistently using e-mail to forward or attach copyrighted material to others and allows this to continue.

**Vicarious Infringement**

**Vicarious infringement** occurs when a company receives direct financial benefit from the infringement by another party and had the right and ability to supervise the infringement activity. Courts have held that vicarious liability requires neither knowledge nor participation in the direct infringement.

In the following case the court dismissed a claim of vicarious liability against an Internet service provider because the plaintiff could not prove any evidence of direct financial benefit received by the provider from posting the infringed material.

---

**Religious Technology Center v. Netcom On-Line Communication Services, Inc.**

*907 F. Supp. 1361 (N.D. Cal. 1995)*

**Facts**

Plaintiffs Religious Technology Center (RTC) and Bridge Publications, Inc. (BPI) hold copyrights in the unpublished and published works of L. Ron Hubbard, the late founder of
the Church of Scientology. Defendant Dennis Ehrlich is a former minister of Scientology turned vocal critic of the church, whose pulpit is now the Usenet newsgroup alt.religion scientology (a.r.s.), an online forum for discussion and criticism of Scientology. Ehrlich posted portions of these copyrighted works on a.r.s. Ehrlich gained his access to the Internet through defendant Thomas Klemesrud’s computer bulletin board service (BBS). Klemesrud is the operator of the BBS, which is run out of his home and has approximately 500 paying users. Klemesrud’s BBS is not directly linked to the Internet, but gains its connection through the facilities of defendant Netcom On-Line Communications.

After failing to convince Ehrlich to stop his postings, plaintiffs contacted defendants Klemesrud and Netcom. Plaintiffs demanded to defendants that Ehrlich be kept off their systems. Klemesrud responded by asking plaintiffs to prove they owned the copyrights to these posted works. Netcom responded that it would be impossible to prescreen Ehrlich’s postings, and that to kick Ehrlich off the Internet meant kicking off the hundreds of users of Klemesrud’s BBS.

Plaintiffs filed suit against Ehrlich, Klemesrud, and Netcom. Issues of Ehrlich’s liability were addressed in a previous court order. That order concluded in part that a preliminary injunction against Ehrlich was warranted. This case continues as to defendants Klemesrud and Netcom. They are named as defendants in this action for copyright infringement. Netcom made a motion for summary judgment. Klemesrud made a motion for summary judgment.

Judicial Opinion (District Judge Whyte)

This case concerns an issue of first impression regarding intellectual property rights in cyberspace.

Cyberspace is a popular term for the world of electronic communications over computer networks. Specifically this order addresses whether the operator of a computer bulletin board service, and the Internet access provider that allows the BBS to reach the Internet, should be liable for copyright infringement committed by a [third party] subscriber of the BBS.

I. Netcom’s Motion for Summary Judgment of Noninfringement

Because the court is looking beyond the pleadings in examining this motion, it will be treated as a motion for summary judgment rather than a motion to dismiss. Summary judgment is proper when ‘the pleadings, depositions . . . show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law.’ The court, however, must draw all justifiable inferences in favor of the nonmoving parties, including questions of credibility and of the weight to be accorded particular evidence.

To establish a claim of copyright infringement, a plaintiff must demonstrate (1) ownership of a valid copyright and (2) ‘copyrighting’ of protectable expression by the defendant. Infringement consists of the unauthorized exercise of one of the exclusive rights of the copyright holder. These rights include the right to reproduce, the copyrighted work, the right to prepare derivative works, the right to distribute copies to the public, and the right to publicly display the work. Plaintiffs argue that, although Netcom was not itself the source of any of the infringing materials on its system, it nonetheless should be liable for
infringement, either directly, contributorily, or vicariously. Netcom disputes these theories of infringement and further argues that it is entitled to its own fair use defense.

The court will address the relevant facts to determine whether a theory of direct infringement can be supported based on Netcom’s alleged reproduction of plaintiffs’ works. The parties do not dispute the basic processes that occur when Ehrlich posts his allegedly infringing messages to a.r.s. Once on Netcom’s computers, [these] messages are available to Netcom’s customers and Usenet neighbors, who may then download the messages to their own computers. Unlike some other large online service providers, such as CompuServe, America Online, and Prodigy, Netcom does not create or control the content of the information. It also does not monitor messages as they are posted. Netcom admits that, although not currently configured to do this, it may be possible to reprogram its system to screen postings. Netcom, however, took no action after it was told by plaintiffs [about] Ehrlich ... instead claiming that it could not shut out Ehrlich without shutting out all the users of Klemesrud’s BBS.

In the present case, there is no question ... that ‘copies’ were created, as Ehrlich’s act of sending a message to a.r.s. caused reproductions of portions of plaintiffs’ works. Even though the messages remained on their systems for at most eleven days, they were sufficiently ‘fixed’ to constitute ... copies under the Copyright Act. Netcom argues that Ehrlich, and not Netcom, is directly liable for the copying. The court believes that Netcom’s act of designing or implementing that [system which] creates temporary copies of all data sent through it is not unlike that of the owner of a copying machine who lets the public make copies with it. [The court thus declines to find] direct infringement. The court does not find workable a theory of infringement that would hold the entire Internet liable for activities that cannot reasonably be deterred.

[The court finds,] [h]owever, the evidence reveals a question of fact as to whether Netcom knew or should have known that Ehrlich had infringed plaintiffs’ copyrights following receipt of plaintiffs’ letter. Thus, it is fair, assuming Netcom is able to take simple measures to prevent further damage to plaintiffs’ copyrighted works, to hold Netcom liable for contributory infringement.

Assuming plaintiffs can prove a violation ... , there is no infringement if the defendant’s use is fair. Congress has set out four nonexclusive factors to be considered in determining the availability of the fair use defense:

1. the purpose and character of the use;
2. the nature of the copyrighted work;
3. the amount ... used in relation to the whole;
4. the effect of the use upon the ... value of the copyrighted work.

In balancing the various factors, the court finds ... Netcom has not justified its copying plaintiffs’ works to the extent necessary to establish entitlement to summary judgment.

[As to Klemesrud,] [t]he allegations [of direct infringement] fail for the same reason. Klemesrud’s computer, not Klemesrud himself, created additional copies. [As for contributory infringement,] [f]or the reasons discusses in connection with Netcom’s motion, the court finds plaintiffs’ pleadings sufficient to raise an issue of contributory infringement. The court denies Netcom’s motion for summary judgment and Klemesrud’s motion for judgment on the pleadings.
Case Questions

1. When did the court say summary judgment is appropriate?
2. What is necessary to establish a claim of copyright infringement?
3. Was it ethical for the court to provide a different standard of liability for Netcom than for other online service providers such as CompuServe, American Online, and Prodigy?

Limitations on Copyright Owners’ Exclusive Rights

Limitations on copyright owners’ exclusive rights include fair use, the first sale doctrine, public domain use, and other statutory exemptions on copyright owners’ exclusive rights.

Fair Use Doctrine

The fair use doctrine is a statutory limitation on the exclusive rights of a copyright owner. Think of fair use as the first cousin to free speech. It is a policy position taken by Congress that the public interest is best served by placing statutory limitations on the copyright owner’s monopoly to its original work. Certain fair uses of a copyright are authorized by law and do not require the consent of the copyright owner. They may even be used over the owner’s objection and are a defense to a copyright infringement lawsuit. For example, limited copyrighted material may be used as handout material in a college classroom over the objection of the copyright owner.

Congress has set out in the Copyright Act (U.S.C. 17, Sec. 107) the following four nonexclusive factors to be considered in determining whether the defense of fair use is appropriate.

1. The purpose and character of the use, including whether its use is of a commercial or educational nature: The first test is to determine if the purpose of the use was commercial or nonprofit educational. In Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417 (1984), the U.S. Supreme Court stated that commercial use of copyright material raises a presumption of unfair use that must be rebutted by the defendant.

Although nonprofit educational institutions that distribute copyright material are inclined to have the benefit of fair use, they must be aware of its limitations. Courts have found copyright infringement for teachers distributing substantial photocopies of portions of books in class and the classroom unauthorized use of videotaped material [Marcus v. Rowley, 695 F.2d 1171 (9th Cir. 1983), and Encyclopedia Britannica Ed. Corp. v. Crooks, 558 F. Supp. 11247 (W.D. N.Y. 1983)].

2. The nature of the copyright material: Courts will examine the nature of the work to determine if it is merely informational or factual. Newsworthy events and mere information are generally subject to fair use.
3. The amount and substantiality of the copyright material in relation to the copyright work as a whole: This criterion is quantifiable and relates to the number of pages used. Distribution of a page or two may be appropriate, but a small critical portion may implicate infringement liability. [Harper & Row Publishers, Inc. v. Nation Enter., 471 U.S. 539 (1985)]. This limitation may be of special importance if a user in a nonprofit institution should download an entire program.

4. The impact of the use on the potential market value of the copyright material: The courts will be unwilling to find fair use if the plaintiff can prove that due to the defendant's copying, the value of the copyright material will diminish. This economic loss can occur either currently or potentially. Even with the first three criteria satisfied, there will not be fair use if the potential market of the copyright material is lost [American Geophysical Union v. Texaco, Inc. 37 F.3d 881 2nd Cir. (1994)].

The U.S. Supreme Court has stated, "Fair use, when properly applied, is limited to copying by others which does not materially impair the marketability of the work copied" [Harper & Row Publishers, Inc., v. Nation Enter., 471 U.S. 539 (1985)].

First Sale Doctrine

The first sale doctrine (Sec. 109(a) of the Copyright Act) limits the copyright owner's exclusive right to distribute publicly a copy of the work when the copyright material was lawfully acquired by another. Under the Copyright Act, "the owner of a . . . copy . . . is entitled, without the authority of the copyright owner, to sell . . . that copy." (17 U.S.C., Sec. 19). You could and probably will sell this textbook, and can do so without violating its copyright. However, the sale, rental, or lease of a licensed computer program without permission of the copyright owner may constitute an infringement.

Consider the case of a textbook purchase in electronic form, transferred and delivered to a student through the Internet. If the student resold the textbook electronically, it would involve the infringing acts of reproduction and public display of the textbook that are not permitted under the first sale doctrine. The first student who owned the book also retained a copy, so the first sale doctrine does not permit the distribution and reproduction of a copy through the Internet.

Public Domain

Materials in public domain are not subject to the exclusive statutory rights of the copyright owner. Public domain falls into two categories: (1) all works of the U.S. government (e.g., the Congressional Record and court decisions), and (2) works whose copyright term has expired (refer back to the explanation of the duration of a copyright).

Other Statutory Exemptions on Copyright Owners' Exclusive Rights

The owner of a copy of a computer program may make a copy as an essential step in using the program in a computer and may make limited copies of that program unless prohibited by the terms of the license (Copyright Act, Sec. 117). See Figure 4.3 for burden of proof in a copyright infringement suit.
FIGURE 4.3  
Burden of Proof in a Copyright Infringement Case

COPYRIGHT INFRINGEMENT LAWSUIT

PLAINTIFF v. DEFENDANT

A. Owner of the registered copyright
B. Violation of an exclusive statutory right under copyright law
C. Theory of liability
   (1) direct infringement
   (2) contributory infringement
   (3) vicarious infringement

Since 1989, under the Berne Convention Implementation Act, there is no longer a requirement that the copyright owner display use of the copyright material by the symbol ©. Although it is now optional, copyright owners should use the circled © with online activities. This will assist the owner in proving that the defendant had knowledge the content was copyrighted.

REMEDIES FOR COPYRIGHT INFRINGEMENT

A plaintiff in a copyright infringement lawsuit has a number of remedies available against the defendant.

1. Monetary damages. The plaintiff may sue for actual damages and for the return of any profits made by the defendant by its use of the copyright material.
2. Statutory damages. If the copyright has been registered in the Copyright Office prior to the commission of the infringement, the plaintiff is entitled to statutory damages in lieu of actual damages. Statutory damages under the Copyright Act are set at $500 to $20,000 per work infringed. Willful infringement may result in damages up to $100,000 per work infringed. Innocent infringement may be reduced to a minimum of $200 per infringed work. Under the Intellectual Property and Communication Omnibus Reform Act 1999, S. 1948, statutory damages will be increased to $750 to $30,000 per work infringed and willful infringement has been raised to $150,000.
3. Attorney’s fees. A successful plaintiff in a copyright infringement case may recover reasonable attorney’s fees from the defendant.
4. Preliminary Injunction (PI) or a Temporary Restraining Orders (TRO). A plaintiff in a copyright infringement case may ask the court for a PI or a TRO in the event there would be irreparable harm in allowing the infringement to continue pending the upcoming trial. This is important because of the long wait before a trial in the federal courts is available.
In 1997, Congress passed the **No Electronic Theft Act**. The statute establishes criminal copyright liability, even without economic gain to the user, when the copyrighted material consisted of one or more works with a total retail value of more than $2,500. The act was based on a 1994 case involving a Massachusetts Institute of Technology undergraduate student who was acquitted of criminal charges after he offered copyrighted software for free on his electronic bulletin board. This is one of many statutes that could make hacking a crime even without economic gain.

**The Digital Millennium Copyright Act (DMCA)**

On October 28, 1998, Title 17 of the Copyright Act was amended by the **Digital Millennium Copyright Act (DMCA)**. Its general purpose is to protect copyright owners from the circumvention of technologies used by them to manage the control and use of the digital content of their copywritten works. The broader purpose of the DMCA is to have the copyright act comply with the World Intellectual Property Organization (WIPO) copyright treaty adopted by many countries.

**Anti-Circumvention of “Digital Locks”**

Digitized material appearing as content on a Web site allows a user to make perfect multiple copies at practically no expense. For example, digitized music, movies, video games, and e-books, unless technologically protected, can be reproduced and sent to countless others in violation of the copyright owner’s exclusive statutory rights. Copyright owners may prevent massive reproductions of their protected works by utilizing software products that provide *technological locks* and controls. The DMCA prohibits a user from decrypting digital locks by circumvention access commonly referred to as the *anti-circumvention provision* [17 U.S.C., sec. 1201 (a)(1)(A)].

**Copyright and Management Systems**

The DMCA prohibits the circumvention of a “digital lock” on a digitized product such as a DVD, e-book, or video game. The statute makes it illegal to “descramble a scrambled work, to decrypt an encrypted work, or otherwise avoid, bypass, remove, deactivate, or impair a technological protection measure” [17 U.S.C. sec. 1201 (a)(2000)]. Companies adopt management systems that utilize “digital locks” on their copyrighted works, thereby denying access to the digitized product. It is now a violation of the DMCA to circumvent this *access control*, including the free distribution of software that might provide such anti-circumvention, or linking to a site with information on anti-circumvention software.

The DMCA provides copyright owners with the right to use circumvention technology that gives them the ability to manage the use of their copyrighted works with respect to how many copies, if any, can be made of the work, how long the copyrighted digitized work will last, or any other control they may wish to place on the reproduction of the original copyrighted work. As software engineers continue to discover ways of controlling digitized products, there is a growing controversy regarding the balance in the copyright act between the rights of the copyright owner and the “fair use” of others.
Trafficking in Circumvention Tools

The DMCA defines the distribution of circumvention tools as “the manufacture, import, offer to the public, to provide or otherwise ‘traffic’ circumvention tools.” This trafficking provision was addressed in a DVD encryption case entitled *Universal v. Corley*, 273 F.3d 429 (2nd Cir. 2001).

In that case, digitized movies have been encoded on digital video discs (DVD) as a copyright management tool to protect the mass distribution of Universal’s digitized products. The defendant, Corley, used a computer program called DeCSS to decrypt the DVD content. The court granted an injunction of the online posting and distribution of DeCSS that was an anti-circumvention software product used to decrypt the DVD movie. One of the troubling questions raised by the case is whether or not merely providing a link to a Web site that contains the anti-circumvention software qualifies as trafficking in an anti-circumvention tool.

**Safe Harbor for Online Service Providers Under the DMCA**

In 1998, Congress codified the online copyright Infringement Liability Limitation Act as Section 512 of the Digital Millennium Copyright Act. The purpose behind the safe harbor is to provide to those entities that qualify as network systems providers federal immunization from claims brought against them by copyright owners based on a theory of secondary liability.

**Online Service Providers (OSPs)**

Search engines, Internet service providers, hosting services, and Web sites with multiple links to third parties provide network access to subscribers and customers who may post materials that infringe on copyrights. In that capacity the customers are direct infringers, violating the copyright owner’s exclusive statutory rights to reproduce the work. The direct infringer is held primarily liable for the infringement.

**Secondary Liability.** However, copyright law also allows claims against secondary infringers under the tort theories of contributory infringement and vicarious infringement. For example, suppose your Web site provides multiple links to other sites that post infringed material as “direct infringers.” Does that linking create potential contributory infringement liability? A contributory infringer is a person or entity that has knowledge of the direct infringement and provides a facility for that infringing process. A vicarious infringer need not have knowledge of the direct infringement but incurs a financial benefit as a result of the direct infringement. Both contributory infringement and vicarious infringement are referred to as secondary liability and represent potential claims by a copyright owner.

**Exemption from Secondary Liability.** These theories of secondary copyright infringement become a significant copyright claim in view of the function of online service providers. So long as the online service providers are in compliance with the DMCA by using proper notification of its policy regarding alleged copyright infringement and
establishing a company agent to be notified in the event of such infringement, they are exempt from secondary liability. This does not mean that entities such as search engines, Internet service providers, hosting services, and Web sites with multiple links can be casual about this exemption. Strict compliance with the DMCA, section 512, is an important function of copyright management by such entities. If the entity qualifies for the DMCA safe harbor exemption, only the direct infringers will be held liable for copyright damages.

**Online Service Provider.** Section 512 (k)(1)(A-B) defines an online service provider as “an entity offering transmission, routing, or providing connections for digital online communications, between or among points specified by a user, or material of the user’s choosing, without modification to the content of the material has sent or received” or “a provider of online services or network access, or the operator of facilities there.”

This vast definition provides a broad umbrella for various entities to function as online service providers. As sophisticated e-commerce Web sites become more and more interactive, the use of search engines, bulletin board systems, chat rooms, instant messaging, and Web sites with multiple links to other Web sites may qualify as online service providers under this broad definition.

An e-business with multiple links to other sites should review with its legal counsel the “safe harbor” provisions of the DMCA to assure compliance in the event of a claim by a copyright owner based on a theory of secondary copyright liability.

**SECTION 512 OF THE DIGITAL MILLENNIUM COPYRIGHT ACT (DMCA) AND THE NAPSTER CASE**

The Digital Millennium Copyright Act was discussed in the Napster case [*A&M Records, Inc., et al. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001)] as a defense argued by Napster. The facts of the case are summarized as follows:

Napster makes music available for free on its web site using MusicShare software. A user downloads this software, then seeks to access the Napster system. Once on the system it reads a list of MP3 files the user has elected to make available to other users and sends that list to Napster’s servers.

If the user wants to locate a particular MP3 file, the user enters the name of the song or band on the search page in the MusicShare program on his/her computer. This software then searches the current directory on Napster’s servers, and generates a list of files responsive to the request. To download one of these files, the user selects that file from the list. The Napster server then communicates this request to the computer on which the file is stored, which request is read by the MusicShare software found on that computer.

Napster moved for partial summary judgment, claiming that DMCA section 512(a) [17 U.S.C. 512(a)] limited the relief that could be awarded against it. Section 512(a) exempts qualifying service providers from monetary liability for direct, vicarious and contributory infringement, and limits the injunctive relief that may be issued by the court.
The court found section 512(a) limits a service provider's liability for copyright infringement by reason of the service provider's "transmitting, routing or providing connections for material through a system or network controlled or operated by or for the service provider." The court held that Napster's role in the transmission of MP3 files by and among the various users of its system was not entitled to protection under Section 512(a) because such transmission does not occur through Napster's system. Rather, all files transfer directly from the computer of one Napster user through the Internet to the computer of the requesting user. Similarly, any role that Napster plays in providing a connection between these two computers does not occur through its system. Said the court:

Although the Napster server conveys address information to establish a connection between the requesting and host users, the connection itself occurs through the Internet. The legislative history of section 512 demonstrates that Congress intended the 512(a) safe harbor to apply only to activities "in which a service provider plays the role of a 'conduit' for the communications of others." . . . Napster enables or facilitates the initiation of connections, but these connections do not pass through the system within the meaning of subsection 512(a).

To be entitled to such protection, a service provider must meet the requirements of section 512(i) of the DMCA, which, among other things, obligates the service provider to "adopt and reasonably implement and inform subscribers and account holders of the service provider's system or network of a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers." The court held that issues of fact existed as to whether Napster had appropriately adopted and informed its users of such an effective policy which precluded at this time any relief to Napster under the DMCA.

**International Regulation and Enforcement of Copyright Law**

A basic international purpose of copyright law is to encourage creativity by recognizing a property right in the artist's creation. The creator of the work should have the power to regulate dissemination of the creation as well as profit from it. Like trademark law, copyright law is generally regulated on a nation-by-nation basis. The following section discusses key issues related to international copyright law and cyberspace.

**Key International Copyright Initiatives**

*The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS).* TRIPS is one of the World Trade Organization's (WTO) multilateral agreements. Like the other WTO multilateral agreements, the WTO member countries are automatically members of the TRIPS Agreement. TRIPS establishes a comprehensive set of rights and obligations governing international trade in intellectual property. To

---

1The text of the TRIPS Agreement is posted at [http://www.wto.org/english/tratop_e/trips_e/trips_e.htm](http://www.wto.org/english/tratop_e/trips_e/trips_e.htm)
accomplish this, the agreement establishes a common minimum of protection for intellectual property rights within the territories of all WTO member countries. The TRIPS Agreement and its relevance to intellectual property law are discussed in more detail in Chapter 3, "Trademarks."

The Berne Convention for the Protection of Literary and Artistic Works (Berne Convention). The Berne Convention creates a union of countries responsible for protecting literary and artistic rights (that is, copyrights). Four principles define the members’ obligations: (1) “National treatment”; (2) “Nonconditional protection” means that no formalities (such as the use of the copyright symbol ©) may be required to protect artistic property; (3) “Protection independent of the country of origin” means that artistic property that is protected in one member country is protected in all; (4) “Common rules” (as with the Paris Convention) establish basic minimum criteria and procedures for granting literary artistic rights.

A great many of the cyberlaw cases heard by courts around the world involved claims of copyright infringement in violation of the national laws that implement the Berne Convention. Examples include the case of Wang Meng v. Century Internet Communications Technology Co., in which a court in Beijing, China, held that the defendant had violated the copyrights of several authors by posting their works on a Web site without their permission, and the case of Int’l Federation of the Phonographic Industry v. Olsson, in which a Swedish court held that a teenager had not infringed any copyrights by posting links to copyright recordings on his Web site.

European Union Copyright Directive (EUCD). The European Union Copyright Directive (EUCD) was formally adopted by the European Parliament on February 14, 2001. The EUCD provides harmonization of copyright protection for rightholders. The EUCD establishes a universal definition of non-commercial private copying. Also, the EUCD authorizes the imposition of penalties against any person who attempts to circumvent security measures from digital files. Article 6 outlaws devices or products “designed to circumvent technological measures” that thwart piracy. The EUCD permits limited replication of copyrighted material for “transient and incidental” reproductions that are an essential part of computer transmission, such as the distribution of files on computer networks. EU members had until summer 2002 to comply with the directive.

WIPO Copyright Treaty (WCT). The WIPO Copyright Treaty (WCT) was adopted in Geneva on December 20, 1996. The WCT builds on the foundation of the Berne Convention, and explicitly states that it does not “derogue from existing obligations” of that convention. The WCT gives copyright holders the power to authorize publication of their works in both wire and wireless modes, in a manner established by the copyright holder. The determination of when infringement occurs is left to the individual member state’s national law. However, Article 12 states that signatories must

---

1The text of the Berne Convention is posted at [http://www.wipo.int/clea/docs/en/wo/wo001en.htm](http://www.wipo.int/clea/docs/en/wo/wo001en.htm)
2Summaries of these cases are posted at [http://www.perkinscoie.com/casedigest/default.cfm](http://www.perkinscoie.com/casedigest/default.cfm)
3The WIPO Copyright Treaty is posted at [http://www.wipo.int/treaties/ip/wct/index.html](http://www.wipo.int/treaties/ip/wct/index.html)
provide legal remedies to copyright holders whose works have been illegally copied through the circumvention of antipiracy technologies. Injunctions and other speedy legal tools must be available to enforce the copyright. Although the WCT requires that signatories develop enforcement measures, the WCT does not have a specific enforcement provision similar to TRIPS.

**WIPO Performances and Phonograms Treaty.** Adopted in Geneva on December 20, 1996, the WIPO Performances and Phonograms Treaty expands on the protection for sound recordings established in prior agreements. Articles 6 through 10 of the treaty give performers the right to control public distribution, manipulation, and rental rights of their works. A record company would have to obtain permission from the performer before distributing the performer’s work under this treaty. Enforcement of these rights is controlled by the legislation of the nation where the performer claims protection.

**Extraterritorial Enforcement of Domestic Copyrights**

Another option for U.S. online firms is to enforce infringement of copyrights abroad through the extraterritorial application of U.S. copyright law. Although U.S. courts rarely allow such application, it may be permitted under certain limited circumstances.

**The U.S. Judicial Reluctance Toward Extraterritorial Enforcement.** A general presumption exists in American law that, unless Congress intends otherwise, legislation passed is only meant to apply within the territorial boundaries of the United States. This is based on the principle that a nation cannot extend its reach beyond its own boundaries. Also, Congress is reluctant to infringe on international law when it enacts domestic legislation. This reluctance becomes particularly important in a cyberspace forum, where online artists are increasingly vulnerable to copying and infringement by anyone around the world with access to the Internet.

The same presumption exists in copyright law. For example, the court in *Subafilms, Ltd v. MGM-Pathe Communications* (1994), considered whether a domestic authorizer of foreign infringement could be held liable for copyright infringement under U.S. law. In 1967, Subafilms and its partner Hearst Corporation entered into agreements with the United Artists, now owned by the defendant, to license and distribute the film *Yellow Submarine*. When the defendant authorized international videocassette distribution of the famous Beatles film, Subafilms and Hearst objected and filed a lawsuit alleging U.S. copyright infringement. The court concluded that the plaintiffs could not sue for U.S. copyright infringement because U.S. copyright law did not extend to conduct engaged in wholly beyond U.S. borders.

**Exceptions to the Presumption Against Extraterritorial Enforcement of U.S. Copyright Law.** Although courts generally refuse to enforce U.S. law for infringements abroad, courts occasionally allow it. For example, in *Steele v. Bulova Watch Co.* (1952), an

---

5The text of the WIPO Performances and Phonograms Treaty is posted at [http://www.wipo.int/treaties/ip/wppt/index.html](http://www.wipo.int/treaties/ip/wppt/index.html)
624 F.3d 1088 (9th Cir.) (en banc), cert. denied, 513 U.S. 1001 (1994).
American citizen named Steele moved his watch manufacturing business to Mexico and registered the mark “Bulova” there. He then assembled watches in Mexico with U.S. parts, stamped the Bulova name on them, and sold them in Mexico. The watches found their way across the border, and the Bulova Watch Company received complaints from jewelers who were being asked to repair the Mexican watches. Even though the infringement occurred in Mexico, the court allowed U.S. law to apply against Steele. The court relied on the facts that Steele purchased parts from the United States, Steele’s watches found their way into the United States, and Steele’s watches adversely impacted the reputation of the Bulova Watch Company. Although this case addressed trademark infringement, its ruling applies with equal relevance to copyrights.

Future courts expanded on the Steele decision and developed a multifactored test to determine whether extraterritorial application is appropriate. In Vanity Fair Mills, Inc. v. T. Eaton Co. (1956), the Second Circuit court identified the following three factors for determining whether the Lanham Act applies to foreign conduct. First, does the defendant’s conduct have a substantial effect on U.S. commerce? Second, is the defendant a U.S. citizen? Third, would extraterritorial application conflict with any trademark rights established under foreign law. These factors have been developed and reshaped by courts over time, but these fundamental elements still apply. If these factors are more or less present, the court will likely permit extraterritorial application of U.S. trademark law.

**Summary**

An e-business’s Web site is a composition of content that is unique and constantly being revised. It represents a large capital investment and must be legally protected from those that would copy and use it without the owner’s consent and payment of royalties. Our legal system provides a process for federal copyright registration of the Web pages that grants the owner exclusive statutory rights. These rights are limited by the fair use doctrine, which has guidelines that must be complied with for the doctrine to be upheld in court.

Because most e-business Web sites have a bulletin board or chat room to interact with the customer, it is important to monitor the material posted to ensure there is no known copyright violation. The e-business could be held liable as a contributory infringer if it knew of the copyright material posted by the customer and actively allowed it to remain online.

---

1. 344 U.S. 280 (1952).
3. Federal courts outside the Second Circuit have developed their own variants of the Vanity Fair Mills test. For example, the Fifth Circuit requires some effect on U.S. commerce for extraterritorial application to apply. See American Rice Growers, 701 F.2d 408 (5th Cir. 1983). The Ninth Circuit has established a more complex multitiered test. See Star-Kist Foods, Inc. v. P.J. Rhodes & Co., 769 F.2d 1393 (9th Cir. 1975). Nevertheless, the fundamental principles established in Vanity Fair Mills almost fifty years ago remain.
An e-business must have its lawyers review and register with the Copyright Office its Web pages. In addition, e-commerce firms must register and protect their copyrights from infringement internationally. Although worldwide enforcement of copyright infringement may have to occur in the nation where the infringement occurred, exceptions do exist that allow a U.S. company to stop infringement of copyright law in other countries in a U.S. court.

Key Terms

- fixed creative work, 87
- Sonny Bono Copyright Term Extension Act (CTEA), 88
- exclusive statutory rights, 91
- derivative work, 93
- public performance, 94
- direct infringement, 94
- contributory infringement, 95
- vicarious infringement, 95
- fair use doctrine, 98
- first sale doctrine, 99
- statutory damages, 100
- No Electronic Theft Act, 101
- Digital Millennium Copyright Act (DMCA), 101
- The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), 104
- Berne Convention, 105
- European Union Copyright Directive (EUCD), 105
- WIPO Copyright Treaty (WCT), 105
- WIPO Performances and Phonograms Treaty, 106
- The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), 104

Manager’s Checklist

- Employee training programs that use videotapes and display Web sites on a computer monitor may be violating the copyright owner’s exclusive right to display the work publicly. Managers should obtain the authorization of the copyright owner.

- When linking to a Web site, consider entering a “Web-linking agreement” with the linked site owner to avoid any possible violation of a Term of Use that may prohibit this practice.

- Web designers and their clients should be careful not to violate the copyright owner’s exclusive right to prepare a derivative work.

- Databases should be arranged in an original and creative manner in order to qualify for copyright registration.

- Managers should be aware of the theories of contributory and vicarious liability.

- Managers should obtain an indemnification contract from the Web site designer in the event of a copyright infringement suit against the company.

- Managers must be prepared to follow the various international copyright laws. This includes mounting a defense of one’s copyright in a non-U.S. judicial forum.

- Managers must anticipate in their contracts with others that international copyright issues may arise. The contract should resolve clearly who holds these copyrights and under what circumstances.
Ethical Considerations

Is it ethical for copyright law to hold a person liable as a direct infringer if she had access to the original copyrighted material and her work was substantially similar? With easy access to the WWW, almost everybody has the original copyright material available. Does that necessarily mean a similar work was copied?

Case Problems

1. Plaintiff Robert Hendrickson, the copyright owner of the documentary “Manson” (dba Tobann International Pictures), filed suit against eBay, an online service provider that “enables trade on a local, national and international basis” for copyright infringement, alleging, among other things, that eBay is liable for the sale of unauthorized copies of the film “Manson” by users on eBay’s Web site. Defendant eBay filed for summary judgment. Decide if “DMCA” offers protection to eBay? What role does the Safe Harbor under Section 512 (c) play here? [Robert Hendrickson, Plaintiff, v. EBay Inc., 165 F. Supp. 2d 1082 (2001)]

2. Plaintiff Leslie Kelly, a professional photographer who has copyrighted many of his images of the American West, licenses those images to other Web sites. Defendant is Arriba Soft Corp., an Internet search engine that displays its results in the form of small pictures. Arriba copied 35 of Kelly’s images to its database without Kelly’s permission and used them on its Web site so users could click on those small picture “thumbnails” to view a large version of the picture. When Kelly discovered this, he brought suit against the defendant for copyright infringement. What critical factors are analyzed in determining whether the use of a particular case is a fair use? Decide if Arriba Soft Corp.’s use of the pictures is a fair use. [Leslie A. Kelly v. Arriba Soft Corporation, 280 F.3d 934 (2002)]

3. Plaintiff Mist-On Systems, Inc. brought a lawsuit against defendants Gilley’s European Tan Spa and Dan Gilley for copyright infringement, claiming the defendant’s Web site FAQ mirrors Mist-On Systems’ FAQ page, resulting in irreparable damage and sustained lost profits, thus seeking monetary relief and a permanent injunction. “To succeed on its copyright infringement claim, plaintiff must show (1) ownership of a valid copyright and (2) copying of constituent elements of the work that are original.” “Unauthorized copying can be established when the plaintiff can show both that ‘the defendant has access to the copyrighted work’ and ‘the accused work is substantially similar to the copyrighted work’.” Decide what test should be used for “substantial similarity.” In order for the court to award attorney fees, what should be done? [Mist-On Systems, Inc. v. Gilley’s European Tan Spa, et al., U.S. Dist., W.D. Wis. (2002)]
4. Plaintiff Harlan Ellison, author of many works of science fiction, is the owner of the copyrights of those works. Defendant Stephen Robertson scanned, uploaded, and copied Ellison's fictional works without Ellison's permission onto his USENET Internet server. USENET is a newsgroup network that shares a variety of topics over its network, including the Internet; AOL became a peer since 1994. By its agreement, one peer's servers automatically transmit and receive newsgroup messages from another peer's server. This data is automatically transmitted to and received by AOL's USENET servers accessible by its users when they reach the particular system through AOL's newsgroup service. By its retention policy for USENET messages, AOL kept the data on the company servers for fourteen days. On April 24, 2000, plaintiff filed suit against AOL and other defendant, alleging copyright infringement and contributory infringement. AOL motioned for summary judgment. Discuss the safe harbor provisions of section 512(a) of the Digital Millennium Copyright Act. Decide. [Harlan Ellison v. Stephen Robertson, an individual; America Online, Inc., et al., 189 F. Supp. 2d 1051 (2002)]

Additional Readings


Business Methods Patents and Trade Secrets

Patents such as yours are the first step in vitiating the Web, in raising the barriers to entry not just for your competitors, but for the technological innovators who might otherwise come up with great new ideas that you could put to use in your own business.

—Letter from Tim O'Reilly, technical publisher to Jeff Bezos, CEO, Amazon.com, January 2000 (see http://www.oreilly.com/ask_tim/amazon_patent.html).

Learning Objectives

After you have read this chapter, you should be able to:

1. Understand the sources of patent law.
2. Summarize the policy reasons for the laws, regulations, and practices.
3. Explain the criteria for granting a patent.
4. Understand the strategies involved in writing patent claims.
5. Understand patent infringement litigation.
6. Understand the sources of trade secret law.
7. Summarize the reasons for these laws and why a business might choose to protect assets through a trade secret strategy rather than through the patent process.
8. Describe the process of protecting assets as trade secrets.
9. Understand how trade secrets are misappropriated.
10. Understand trade secret litigation.
11. Understand international issues related to business methods patents.
12. Understand the challenges of protecting trade secrets on a global scale.

Introduction

The patent system of protection for inventions is recognized in the U.S. Constitution. As with copyrights, the power to grant patent protection resides with Congress. It represents an effort "to promote the progress of science and useful arts, by securing for limited times in authors and inventors the exclusive right to their respective writings and discoveries."
The patent system was designed to act as an important incentive for inventors. It was also construed as an important engine for the development and growth of new technologies, and thus a direct link to the improvement of the domestic economy. These considerations have not changed over the last two centuries, yet what has changed is the content and character of the inventions and creations. Now, instead of patenting improvements to the making of pot ash and pearl ash (essential ingredients for making soap, glass, dyeing fabrics, baking, saltpeter and gunpowder, and other such tangible products—see U.S. Patent Number 1), we see patents for business processes and software programs, such as one-click ordering systems (Amazon), micro-payment methods (PayPal), and online auction software (eBay). Although there are various classes of patents (including utility, design and plant patents), we focus on business methods patents only (a subclass of utility patents), because of their high relevance to e-commerce. We examine what business methods are patentable and how patent infringement claims are litigated.

Trade secrets, another method of protecting digital intellectual property assets, are perhaps the least understood and the most used. Essentially, a trade secret strategy requires the establishment and maintenance of the secret, a continuous managerial effort. The trade secret need not be novel, obvious, or useful, and the secret carries on indefinitely, potentially beyond the limited term of patent protection. Thus the protections of trade secrets can be broader and longer than patents, yet are perhaps more susceptible to theft and misappropriation. We look at how trade secrets are developed and managed. Finally we examine how claims are litigated.

**Business Methods Patents**

**Legal Framework of Patents**

By way of background, it is helpful to describe what a patent is, and is not, before we discuss its relevance to e-commerce and cyberspace law. A patent is the grant of a property right to inventors by the U.S. Patent and Trademark Office (USPTO) for an invention, for a term of twenty years from the date on which the application was filed. It is, in essence, a government-sponsored monopoly to recognize and reward inventors by granting inventors exclusive control of the patent subject matter. The grant of a patent gives inventors the right to exclude others from making, using, offering for sale, or selling the invention. It is not the right to make, use, offer for sale, or sell the invention—although these possibilities of commercialization are available to patent holders. The legal environment of patent laws consists of the interplay of the Constitution, congressional enactments, agency interpretation of those laws, and judicial review of those laws as applied to commercial transactions.

**U.S. Constitution.** Article 1, Section 8, of the U.S. Constitution is the source of patent regulation. It states, “Congress shall have power . . . to promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries.”

The regulation of patents is a constitutional grant of power to Congress to create a federal law of patents. Congress has the exclusive power to make all laws relating to
Chapter 5 Business Methods Patents and Trade Secrets

patent review and administration, including the length of term for the protection of patented inventions. This power preempts state legislation and regulation. The patent system is meant to create economic incentive for entrepreneurship and inventiveness. The primary goal of patent laws is to create an incentive to innovate through the conferral of a monopoly. This secures the invention for the benefit of the public and advances the useful arts and sciences. Secondarily, patent laws are designed to be a barrier to theft. Thus the term becomes sort of an economic balancing act: the term granted is meant to motivate and repay inventors and act as a complete, but temporary barrier to entry. The original length of patent protection granted was set at four years. The first patent examiner, Thomas Jefferson, was conflicted over the patent system. Although his goal was to promote inventions, he was dismayed by the system’s collateral effect of promoting protection. This debate continues today.

**Congressional Powers.** Under this constitutional grant of power, Congress possesses the power to regulate patents. Pursuant to this, it has enacted patent laws, beginning in 1790, and most notably, it enacted the modern law through the Patent Act of 1952. (Congress later incorporated other statutes into this act, including the American Inventors Protection Act and Patent Cooperation Treaty.) Congress has delegated oversight power to the U.S. Patent & Trademark Office (USPTO).

**Patent Act** The Patent Act is the main patent statute, providing among other things, that “whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefore, subject to the condition and requirements of” this statute. (These requirements are discussed in detail later.) In essence, the Patent Act makes a bargain with inventors: in exchange for complete information on the invention, it grants a monopoly. Thus all secrets in the process are turned over for public review and scrutiny—and are helpful to competitors. (This is in contrast with a strategy of protecting information under the trade secret laws, wherein nothing is publicly revealed.)

Also, as with copyright protection, the term of protection has increased over the years. Congress extended the original four-year term length to fourteen years; and again extended it to its current term of twenty years (for utility and plant patents only; design patents have a term of fourteen years). The length of the term is (or if not, it should be) calculated to maximize these values, but also, not so overly long as to be oppressive, thus thwarting the very innovation it was intended to promote. Critics assert that the present overly long patent protection is oppressive and counter to the Framers’ intent. This debate has a parallel in copyright law, with respect to the recently decided *Eldred v. Ashcroft* case challenging the Copyright Term Extension Act. (See Chapter 4, “Copyrights,” for an explanation of the *Eldred* case.)
American Inventors Protection Act of 1999

The American Inventors Protection Act is a series of amendments to the Patent Act that are intended to strengthen an inventor's rights in relation to other later inventors and patent promotion companies. It also strengthens third parties' right to examine and comment on patent applications. The act guarantees a minimum term length of protection, sets application fees, creates study commissions, and so forth.

Agency Enforcement of Patent Laws

USPTO. The USPTO administers the patent laws, examines new applications, grants patents, publishes issued patents, publishes applications for patents, records assignments of patents, and maintains a database in order to search patents. The USPTO site offers a range of services and invaluable information on the patent process.

Courts. Courts are the final authority on patent matters. A special judicial framework has been created in order to construe patent laws uniformly and resolve patent disputes. A separate circuit court, the Court of Appeals for the Federal Circuit, hears all patent appeals. Any appeals from this circuit are heard by the Supreme Court. Patent suits usually involve a range of issues; many include challenges to inventorship, validity, misuse, and infringement.

Patent Law as It Relates to Business Practices

Patentable Subject Matter

The Patent Act specifies what may be patented. The three main requirements are set forth here. Historically, patent subject matter pertained to physical inventions. The patent subject matter of today is much more abstract. In an information economy, where assets are in digital format, inventors are understandably interested in protecting their investment in creating those assets, and later, ensuring a return on them. Examples of such inventions include innovations from R&D labs in software development, computer science, robotics, artificial intelligence, biotechnology, life science, and genetics. The exploitation of these assets and commercialization of such inventions depends in large part on the patent system where patent owners may develop the process into commercial products or services, and even transfer or license the process to others.

What is deserving of a patent: the requirements:

An invention or discovery (such as of a machine, article, process, or composition) that is:

- Novel;
As simple as this definition seems, these issues continue to be litigated.

**An Invention or Discovery.** An invention or discovery is patentable if it produces a “useful, concrete and tangible result” [*State Street Bank & Trust Co. v. Signature Financial Group, Inc.*, 149 F.3d 1368 (1998)]. This is construed to “include anything under the sun that is made by man” [*Diamond v. Chakrabarty*, 447 U.S. 303, 309 (1980)]. Inventions and discoveries may be related, to both natural and human-made creations.

Inventions that are not patentable are “laws of nature, natural phenomena, and abstract ideas” [*Diamond v. Diehr*, 450 U.S. 175, 185 (1981)]. These include the following:

- purely mental processes/abstract ideas,
- naturally occurring phenomena, and
- scientific laws.

Exceptions to this rule of no patentability are when these things produce a useful result. For example, an application of abstract ideas (not just pure math) is patentable subject matter. See *In re Alappat*, 33 F.3d 1526 (Fed. Cir. 1994) (*en banc*). So, whereas the sun itself is not patent subject matter, a use of the sun, such as the design and manufacture of photovoltaic cells that transform sunlight into energy, may be patent subject matter. (Finally, patents are not allowed for inventions useful solely for nuclear and atomic weapons.)

**Novel.** The invention must not have been invented, patented, or published before. This requires that this particular invention was never patented before the inventor invented it; never before described in a publication; and never before in public use or for public sale more than one year preceding the date on which an application for a patent was filed.

When there is this prior art, the invention is not patentable. Currently, there is a trend by those critical of the patenting process to “defensively publish” a description of the invention on the Web before it is patented by the inventor. This creates prior art and thereby deprives inventors of the opportunity to patent the invention. Prior art may be found in the USPTO site, trade publications, books, journals, and conference proceedings. Novelty is a fiercely contested issue in business methods patent litigation.

**Useful.** This requires that somehow the invention operates/does/performs/accomplishes something useful. It has to have a practical benefit, in fact anything whatsoever. (This is not construed to mean the invention must have a commercial/marketable application.)
The limits of “useful arts” is not known at this time. The USPTO has deemed the following two examples useful—and thus patentable subject matter.

1. U.S. Patent 5,443,036: Method of exercising a cat

Abstract

A method for inducing cats to exercise consists of directing a beam of invisible light produced by a hand-held laser apparatus onto the floor or wall or other opaque surface in the vicinity of the cat, then moving the laser so as to cause the bright pattern of light to move in an irregular way fascinating to cats, and to any other animal with a chase instinct.

2. U.S. Patent 5,993,336: Method of executing a tennis stroke

Abstract

A method of executing a tennis stroke includes covering a knee of a tennis player with a knee pad during tennis play. The covered knee of the player is placed on a tennis court surface with the knee pad positioned between the knee and the surface. The tennis racket is swung toward a tennis ball so as to hit the tennis ball with the racket either while the covered knee is on the tennis court surface, or just prior to the knee contacting the tennis court surface.

There are many such inventions as these that have been awarded patents, too.

Nonobvious. This is the inventive step that takes the patent subject matter out of the realm of the obvious and easily anticipated. This requires that the invention must not be obvious/anticipated to a person having ordinary skill in the particular field of invention. An invention is not patentable if the differences between the invention and the prior art are such that the invention would have been obvious. For example, a civil engineering innovation in bridge building is not patentable if it is mere substitution of one material for another or just changes in dimensions. It has to amount to an “inventive step,” an innovation that is not obvious to the average civil engineer.

This issue of nonobviousness is also hotly contested with regard to business methods patents, where critics note that many of these Internet applications (of such commonplace events as shopping and browsing) could have been easily anticipated and were an obvious next step given the direction of e-commerce, rather than an inventive step.

To assure that an invention is patentable, therefore, it is extremely important to make a detailed, thorough research effort, utilizing patent as well as nonpatent literature (such as trade magazines and sites), in order to determine whether this subject matter is new, useful, and nonobvious.
In a recent case, Trilogy Software sued CarsDirect over U.S. Patent No. 5,825,651 covering a system for choosing options when buying a car online. This would seem to cover the mere automation of the car salesperson's job. In another recent case, SightSound sued NsK over U.S. Patent No. 5,191,573 covering online sales of music. This would seem to be an easily anticipated new application of the present way of conducting music sales.

**Types of Patents**

There are three classes of patents: *utility patents* (new and useful process, machine, article of manufacture, compositions of matter, or improvements thereof—this class includes business methods patents); *design patents* (new, original, and ornamental design for articles of manufacture); and *plant patents* (inventions or discoveries relating to reproducing any distinct and new variety of plants). Because business methods patents are the only ones directly related to the focus of this text, the Internet and e-commerce, we limit our discussion to this one subclass of patents.

**What Claims Are Covered**

The value of a patent depends on many factors, including how inventive it is. But more particularly, the writing of the claims is of critical importance. In patent applications, inventors describe exactly what the patent, if issued, would cover in detail. The Patent Act requires inventions to describe their work in "full, clear, concise, and exact terms" [35 U.S.C. section 112]. A patent agent or attorney states in the application the broadest possible statement of the invention first—that will cover the most claims. Then the parties progress through a restatement of the claims in an effort to narrow, or reduce, the number of claims the patent holder will ultimately control. To the extent the Patent Office allows more claims, the patent is broader. In fact, the reach of the patent may extend beyond even those claims granted, by virtue of the judicially created doctrine of equivalents—that excludes inventions that are a copy, or "equivalent" to the patented ones.

**First to Invent versus First to File a Patent**

This issue arises when two inventors file a patent on the same invention at the same time. Under the first-to-invent system, the one who invented the process earliest wins. Under a first-to-file system, the one who files earliest wins.

The U.S. Patent Office, since its inception over two centuries ago, worked on a first-to-invent system. Under this system, inventors need only keep records of their inventions as they make progress. Inventors have time to make refinements, get feedback, and generally mature the invention. All of this is done before filing for patents. This system, by its nature, favors inventors, inventiveness, and innovation.

Under a first-to-file system, there is an incentive to rush and file the application. First-to-file rules discourage feedback and discourse among inventors and instead create an atmosphere of secrecy lest another inventor wins in the race to file. This
system favors large organizational entities with a corps of support staff. This system though, is simpler and greatly reduces interferences, a process that is declared when there is a dispute over who is the first to invent the process. The European Community and other states follow the first-to-file system, and so it is likely the United States will adopt this system in order to harmonize American intellectual property laws with those of Europe.

**THE PATENTABILITY OF SOFTWARE AND BUSINESS METHODS PATENTS**

**Software Patents**

In 1981, the Supreme Court first recognized the patentability of software in the *Diamond v. Diehr* case. In this suit the Court was asked to consider whether a process for curing synthetic rubber employing a mathematical formula and a programmed digital computer is patentable subject matter under the Patent Act. (Previously this process was done by employees regularly checking the temperature of the rubber. The company came up with an algorithm that would more precisely do the same job.) In this case, the patent examiner rejected the application because it involved an algorithm, which was historically not patentable subject matter. In a 5–4 decision, the Court rejected this approach, instead deciding it was patentable subject matter. It reasoned that the process created a new useful and nonobvious result. (The Court cautioned, however, that the algorithm, by itself, was a nonpatentable abstract idea and not inherently useful.) The Court reaffirmed that patent law is not confined to new machines or compositions of matter, but extends to any novel, nonobvious, and useful art, process, or manufacture—even software.

Recall in Chapter 4 that we discussed the copyright protection available for software. There is an overlap between patent and copyright law as they relate to software development. Software programs consist of both language and function. To the extent the software expresses ideas (through source code), it may be copyright protected. To the extent it produces a new, useful, and nonobvious result (through object code), it is patentable subject matter. (For a case applying these concepts, see the *Universal Studios, Inc. v. Corley* case in Chapter 11. That case involves a decryption program that circumvents the code written into DVDs.)

Software patents are reaching into areas that are almost incomprehensible today—with the realities of animal cloning firmly established and the possibility of human cloning on the horizon. By patenting DNA code of living organisms and living animals with engineered genetic codes, the range of patentable subject matter is perhaps exceeding the public good. *Diamond v. Diehr* paved the way for consideration of another expansion of the range of patentable subject matter—business methods patents.

Justice Stevens's dissent in *Diamond v. Diehr* is important and relevant to our discussion today over what a business methods patent is and whether it is statutory subject matter. He makes several points. Most notably, he found that the process was merely a high-tech rendition of what the company had already been doing—that
is, curing rubber. So, in effect, the transference of the job from a manual system to an automated one was neither new nor nonobvious. No inventive concept was disclosed/introduced beyond the algorithm; the process was the same, and this one minor change was easily anticipated. He considered this not to be patentable subject matter, therefore. Second, he questioned the merits of the majority's decision because no rules have been established for the patentability of program-related inventions. If there are no standards, how can the law develop in any rational way?

**Business Methods Patents**

With the patentability of software established and widespread recognition of the utility of computer programs to accomplish a variety of tasks, it became a matter of time before the question arose over the patentability of business methods. As Justice Stevens pointed out, there are no firm rules for these patents, and to exacerbate the situation, there is no precise definition. **Business methods patents** are considered to include any process involving data processing, calculations, conversions, and so on, used for business operations and management.

The USPTO groups them with the class of patents known as utility patents that protect inventions and formulae, and defines them as follows:

**Class 705**

**DATA PROCESSING: FINANCIAL, BUSINESS PRACTICE, MANAGEMENT, OR COST/PRICE DETERMINATION**

**Class Definition:**

This is the generic class for apparatus and corresponding methods for performing data processing operations, in which there is a significant change in the data or for performing calculation operations wherein the apparatus or method is uniquely designed for or utilized in the practice, administration, or management of an enterprise, or in the processing of financial data. This class also provides for apparatus and corresponding methods for performing data processing or calculating operations in which a charge for goods or services is determined.

The leading case establishing that business methods are patentable subject matter is *State Street Bank & Trust*. Again, courts had to consider the breadth of the Patent Act and whether it encompassed a conceptual process: a business method that made use of algorithms to transform data. The result of this case is to abolish a hundred years of law holding that business methods patents were not patentable subject matter. This case greatly expands the universe of subject-matter patentability. This case will always be a benchmark and reference point (and poster case) for the controversial issues surrounding business methods patents.

| http:// | To read the entire definition, see http://www.uspto.gov/web/offices/ac/ido/oeip/taf/def/705.htm
| To read insightful commentary, visit http://www.bustpatents.com
| http://www.patnewsinc.com/
| http://www.cptech.org/ip/business/
| http://www.oreillynet.com/policy |
State Street Bank & Trust Co. v. Signature Financial Group, Inc.

Facts

Signature is the assignee of U.S. Patent No. 5,193,056 (the '056 patent), which is entitled “Data Processing System for Hub and Spoke Financial Services Configuration.” The '056 patent issued to Signature in 1993 named R. Todd Boes as the inventor. It is generally directed to a data processing system for implementing an investment structure developed for use in Signature’s business as an administrator and accounting agent for mutual funds. The system facilitates a structure whereby mutual funds (the Spokes) pool their assets in an investment portfolio (the Hub) organized as a partnership. It determines the percentage share that each Spoke maintains in the Hub, as well as daily changes in net asset value. Additionally it tracks all relevant data for tax purposes. This investment configuration provides the administrator of a mutual fund with the advantageous combination of economies of scale in administering investment coupled with the tax advantages of a partnership.

Speed and accuracy in calculation are essential for this system because shares in the investments are sold to the public and quoted daily. A computer is a virtual necessity to perform these complex tasks. Thus the claims encompass a machine (definitely patentable subject matter) as it relates to a business method (hertofores questionable whether it is patentable subject matter).

State Street and Signature are both in the business of acting as custodians and accounting agents for multitiered partnership fund financial services. State Street negotiated with Signature for a license to use the '056 patented data processing system. When negotiations broke down, State Street brought a declaratory judgment action asserting invalidity, unenforceability, and noninfringement. The federal district court held for State Street, and Signature appealed.

Judicial Opinion (Judge Rich)

The substantive issue on hand, whether the '056 patent is invalid for failure to claim statutory subject matter under section 101, is a matter of both claim construction and statutory construction. Claim 1, properly construed, claims a machine, namely, a data processing system... which machine is made up of... specific structures disclosed in the written description and corresponding to the means-plus-function elements.

This does not end our analysis, however, because the [trial] court concluded that the claimed subject matter fell into one of two judicially-created exceptions to statutory subject matter. The first exception [is] the ‘mathematical algorithm’ exception and the second exception [is] the ‘business method’ exception. Section 101 reads:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may
obtain a patent therefore, provided it meets the other requirements for patentability set forth in Title 35.

[Section 101 specifies that statutory subject matter must also satisfy the other ‘condition and requirements’ of Title 35, including novelty, nonobviousness, and adequacy of disclosure and notice.]

The plain and unambiguous meaning of section 101 is that any invention falling within one of the four stated categories of statutory subject matter may be patented. The use of the expansive term ‘any’ in section 101 shows Congress’s intent not to place any restrictions on the subject matter for which a patent may be obtained beyond those specifically recited in section 101. Indeed, the Supreme Court has acknowledged that Congress intended section 101 to extend to ‘anything under the sun that is made by man.’

The “Mathematical Algorithm” Exception

The Supreme Court has identified three categories of subject matter that are unpatentable, namely ‘laws of nature, natural phenomena, and abstract ideas.’ Of particular relevance to this case, the Court has held that mathematical algorithms are not patentable subject matter to the extent that they are merely abstract ideas. To be patentable an algorithm must be applied in a ‘useful’ way. [For example] in Alappat, we held that data transformed by a machine through a series of calculations to produce a smooth waveform display on a monitor, constituted a practical application of an abstract idea.

Today, we hold that the transformation of data, representing discrete dollar amounts, by a machine through a series of mathematical calculations into a final share price, constitutes a practical application of a mathematical algorithm, because it produces a ‘useful, concrete and tangible result’—a final share price—[and thus it is] statutory subject matter.

The question of whether a claim encompasses statutory subject matter should not focus on which of the four categories of subject matter a claim is directed to—process, machine, manufacture, or composition of matter—but rather on the essential characteristics of the subject matter, in particular, its practical utility.

The “Business Method” Exception

As an alternative ground for invalidating the ‘056 patent under section 101, the [trial] court relied on the judicially-created, so-called ‘business method’ exception to statutory subject matter. We take this opportunity to lay this ill-conceived exception to rest. [A business method] is as patentable as anything else, and is not in fact, any exception to patent law at all. Business methods are always patentable subject matter, provided they meet the other requirements of the statute. Claim 1 is therefore statutory subject matter—a business method that is patentable. Whether the claims are directed to subject matter within section 101 should not turn on whether the claimed subject matter does ‘business’ instead of something else.

REVERSED.
Case Questions

1. Why were algorithms historically not patentable?
2. What are Signature’s business options following this opinion?
3. What are State Street’s business options following this opinion?

The State Street Bank & Trust case therefore recognized the validity of both software patents and business methods patents, and it paved the way for Internet-related patents, including software for databases, shopping rewards, ordering systems, reverse auctions, incentive programs, and so forth.

Immediately following the State Street Bank & Trust case, the Federal Circuit decided AT&T Corp. v. Excel Communications, Inc., 172 F.3d 1352, cert. denied, 528 U.S. 946 (1999). This case involved a “Call Message Recording for Telephone Systems.” The court once again examined the scope of the Patent Act and found the claimed subject matter—here, a mathematical algorithm that transformed data—and held it was patentable subject matter.

The result of these two cases has been an explosion in the number of these conceptual patents on business practices, and questions are being raised about the quality of these patents that the USPTO is granting. Moreover, this decision prompted a change of tactics by Internet businesses, the majority of which heretofore protected business methods with a trade secret strategy. Patenting business methods became a viable and appealing alternative to trade secrets, because patent protections carry on even when trade secret protection is lost because of such events as reverse engineering or public disclosure of the secrets.

What May Be Done with the Patent

Patent Commercialization and Knowledge Transfer Strategies. A patent does not in and of itself represent any return on investment. That is up to the patent owner to make business decisions on how best to exploit the value of the claims covered by the patent. The mere fact of ownership of a patent creates two values. One is the financial/monetary/market value in the patent property itself. The other related value is the monopoly effect. The value of owning a certain property, the first of its kind, is in knowing you may exclude all others. It is a land grab of sorts, albeit temporary. This creates huge barriers to entry, where patent owners have an enormous competitive advantage. How a patent is utilized is a pure business decision, whether and how to create value with the patent. Other strategies for patent use include technology transfers, assignments, and licensing. These create revenue for the inventors with somewhat less risk.

Note too, how patents relate to business valuation. It is quite a challenge to value intangible assets such as these, as they are susceptible to rapid and dramatic changes, and they have a limited lifetime of up to only twenty years. In the 1950s, for example,
tangible assets represented 78 percent of the assets of U.S. nonfinancial corporations. In 2002, the proportion is 53 percent. This has contributed to market volatility and has created a great deal of market uncertainty as to how much assets are worth [Greg Ip, “The Rise and Fall of Intangible Assets Leads to Shorter Company Life Spans,” Wall Street Journal (April 4, 2002), p. 1].

**Shop Rights and Ownership of Patents.** Inventorship and ownership of patents are separate statuses. For the most part, patents are owned by the inventors, but these rights may be assigned, licensed, or transferred. Complex issues arise when inventorship is unclear or the duties to assign are not clear. The patent application must be filed in the name of the inventor. Whether inventors are obligated to assign their patents to employers, unless there is a contractual agreement to do so, can become a major issue.

The shop rights issue arises when an invention is invented by an employee who is under no duty to assign patent ownership but developed the invention using employer resources. Employers enjoy a shop right in the patent, entitling them to a royalty-free nonexclusive license to the patent.

Other issues arise, such as in cases where coinventors are working together, but located in different places and working on different aspects of the same process. The best method of avoiding all of these possibilities is for businesses to include within their employment agreements policies outlining resource allocation, development and ownership of inventions, creations, and trade secrets.

The following case is a challenge to inventorship, involving one of the best known business methods patents, and the case shows how even seemingly simple questions become muddled in the Patent Office.

**Marketel International, Inc. v. Priceline.com**  
*138 F. Supp. 2d 1210 (N.D. Cal. 2001)*

**Facts**

Plaintiff claims that its employees, Perell, Martinez Hughes-Hartogs and Weiss (the *alleged* inventors), were the *actual* inventors of the business method and apparatus claimed in U.S. Patent No. 5,794,207 (the ‘207 patent) that was registered by Priceline. Plaintiff asserts that the alleged inventors explained the substance of their inventions to agents of defendants in confidential documents and conversations—before defendants sought and received a patent on the disputed invention. Plaintiff seeks relief in the form of an order correcting inventorship in the ‘207 patent so plaintiff’s employees are added to the certificate naming inventorship, as the only inventors.

Defendant motioned for summary judgment arguing that (1) plaintiff’s asserted conception of the subject matter is not corroborated; and (2) plaintiff’s asserted communication of the invention to defendants is not corroborated.
U.S. Patent No. 5,794,207:

‘Method and apparatus for a cryptographically assisted commercial network system designed to facilitate buyer-driven conditional purchase offers’

The Abstract of the Invention:

The present invention is a method and apparatus for effectuating bilateral buyer-driven commerce. The present invention allows prospective buyers of goods and services to communicate a binding purchase offer globally to potential sellers, for sellers conveniently to search for relevant buyer purchase offers, and for sellers potentially to bind a buyer to a contract based on the buyer’s purchase offer. In a preferred embodiment, the apparatus of the present invention includes a controller which receives binding purchase offers from prospective buyers. The controller makes purchase offers available globally to potential sellers. Potential sellers then have the option to accept a purchase offer and thus bind the corresponding buyer to a contract. The method and apparatus of the present invention have applications on the Internet as well as conventional communications systems such as voice telephony.

The Listed Inventors are: Walker; Jay S. (Ridgefield, CT); Schneier; Bruce (Oak Park, IL); Jorasch; James A. (Stamford, CT)

The Patent was assigned to: Walker Asset Management Limited Partnership (Stamford, CT)

35 U.S.C. section 256 authorizes federal courts and the PTO to resolve inventorship contests. Inventors may be added, and there may be a complete substitution of one inventor for another. The person name in an issued patent is presumed to be the true inventor. This presumption is a powerful one, and the burden of showing misjoinder or nonjoinder of inventors is a heavy one, and must be proved by clear and convincing evidence.

Judicial Opinion (Judge Legge)

It is axiomatic that ‘conception is the touchstone of inventorship.’ Conception is the formation in the mind of the inventor, of a definite and permanent idea of the complete and operative invention, as it is hereafter to be applied in practice. Thus, facts relevant to inventorship are those showing the conception of the invention, for others may provide services in perfecting the invention conceived by another without becoming an ‘inventor’ by operation of law. To establish priority of invention, a party must show: (1) possession of every feature recited in the disputed claim; and (2) every limitation of the claim was known to the inventor at the time of alleged invention. To establish that the named inventor derived the invention from another, a party must show: (1) prior conception of the claimed subject matter, and (2) communication of the conception to the named inventor. The determination of whether there was a prior conception is a question of law.

An inventor’s testimony ... cannot, standing alone, rise to the level of clear and convincing proof. An alleged inventor must supply independent evidence to corroborate the essential aspects of his testimony. [Here] Plaintiff asserts that the alleged inventors
explained the substance of their inventions to agents of Defendant in confidential documents and conversations before Defendants sought and received a patent on the disputed invention. Plaintiff argues that 'numerous Marketel documents corroborate Marketel witnesses' account of the process by which Marketel invented and developed the trade secrets misappropriated by Defendants. But instead of presenting this evidence and relating it to the elements of the cause of action, Plaintiff merely states that such evidence has been 'described in great detail.'

Plaintiff's showing is insufficient. When the moving party (Defendant—for summary judgment) points to an absence of proof and the nonmoving party will bear the burden of proof . . . the nonmoving party must . . . 'designate specific facts showing that there is a genuine issue for trial.' Plaintiff has designated no specific facts. Even if the court were to agree [with Plaintiff] that there is a 'remarkable correlation' between Defendants' patent claims and Plaintiff's alleged trade secrets, this does not address (1) which of the particular claims . . . were conceived by the alleged inventors; (2) the timing of the alleged inventors' purported conception; (3) communication of the alleged inventors' supposed inventions to Defendants'; or (4) the individual contributions, and therefore the basis for the claims to inventorship. General reference to . . . declarations of [parties do not] carry the day. The court is not obliged to sort through all of Ps declarations to locate evidence on its behalf. Given that the record on these summary judgment motions measures at least six feet in height, the concerns addressed . . . are very real here.

[Finally finding some documentation, the court then decides] the declaration of Martinez and Perell, CEO and CFO of Marketel respectively, begin to flesh out the history of Marketel and its innovative business method plans from its inception. At first blush, this appears to be the type of evidence required. On closer inspection, however, this is only the undeveloped germ of an inventorship correction claim [as the documents relate mainly to private placement documents and short, and long-term plans]. Without more, this does not establish the existence or communication of a 'definite and permanent idea of the complete and operative invention' needed to support prior conception. The testimony from two of the alleged inventors is insufficient to raise a triable issue, and there is insufficient corroborative evidence to substantiate their claims.

The court GRANTS summary judgment in favor of Defendants, for inventorship correction.

IT IS SO ORDERED.

Case Questions

1. Do plaintiffs have any other possible cause of action after this case?
2. What is the significance to Priceline of actually owning, rather than licensing, this patent?
3. Say plaintiffs invent some refinements to the '207 patent. Should they seek a patent on these?
ENFORCING PATENT RIGHTS: PLAINTIFF’S CASE

Businesses need to keep abreast of their products and services in the marketplace, and there is even more incentive to do so where the assets have the additional protections of a patent. To enforce rights of control that a patent affords, there are two theories of patent infringement that plaintiffs may allege.

Literal Infringement

Under the Patent Act, infringement is defined as one who makes, offers, uses, offers to sell, or sells any patented invention, or actively induces infringement on any of the claims covered by the patent. Patent litigation is a civil matter. Importantly for plaintiffs, there is a presumption that a patent is valid. The statute allows for equitable relief, as well as damages for any infringement. Damage claims may include lost profits on lost sales, price deterioration, lost royalties, and lost licensing opportunities.

The following decision is perhaps the most notorious of the business methods patent cases. Although litigation carried on even after this decision, the parties settled the matter in 2002. This case remains important reading regarding issues of literal patent infringement and validity, how the patent process works, and the necessity of checking on the existence of prior art.

Amazon.com, Inc. v. Barnesandnoble.com, Inc.
239 F.3d 1343 (Fed. Cir. 2001)

Facts

This case involves U.S. Patent No. 5,960,411 (the '411 patent) which issued on September 28, 1999, and is assigned to Amazon. On October 21, 1999, Amazon brought suit against barnesandnoble.com (B&N) alleging infringement of the patent and is seeking a preliminary injunction.

Amazon’s Patent: ‘A method and system for placing an order to purchase an item via the Internet.’

Patent Abstract:

The order is placed by a purchaser at a client system and received by a server system. The server system receives purchaser information including identification of the purchaser, payment information, and shipment information from the client system. The server system then assigns a client identifier to the client system and associates the assigned client identifier with the received purchaser information.
The server system sends to the client system the assigned client identifier and an HTML document identifying the item and including an order button. The client system receives and stores the assigned client identifier and receives and displays the HTML document. In response to the selection of the order button, the client system sends to the server system a request to purchase the identified item. The server system receives the request and combines the purchaser information associated with the client identifier of the client system to generate an order to purchase the item in accordance with the billing and shipment information whereby the purchaser effects the ordering of the product by selection of the order button.

Inventors: Hartman; Peri (Seattle, WA); Bezos; Jeffrey P. (Seattle, WA); Kaphan; Shen (Seattle, WA); Spiegel; Joel (Seattle, WA)

Assignee: Amazon.com, Inc. (Seattle, WA) Appl. No.: 928951

Amazon developed the patent to cope with what it considered to be frustrations presented by what is known as the ‘shopping cart model’ purchase system for e-commerce transactions. That model required a number of steps to perform several actions before achieving the goal of a placed order. The '411 patent sought to reduce the number of actions required from a consumer to effect a placed order; such that only a single action needs to take place after the products are chosen. The '411 patent has 26 claims, 4 of which are independent; some are for method, others are for apparatus. B&N developed a standard shopping cart system, and another system, called the Express Lane, which it consistently advertised as a 1-click ordering system. [Incidentally, B&N trademarked the name ‘Express Lane’.] B&N began using the Express Lane system in May 1998.

The trial court granted Amazon’s request for a preliminary injunction enjoining B&N from using any feature of the '411 patent, finding it likely that there was infringement. [They reached this decision in spite of some evidence of prior art.] B&N’s appeal attacks the trial court’s decision on two grounds: that either its method does not infringe the ‘single action’ limitation—or that the ‘single action’ feature of the patent is invalid.

Judicial Opinion (Judge Clevenger)

Both infringement and validity are at issue in this appeal. It is well settled that an infringement analysis involves two steps: the claim scope is first determined, and then the properly construed claim is compared with the accused device to determine whether all of the claim limitations are present either literally or by a substantial equivalent. [T]he first step of an invalidity analysis based on anticipation and/or obviousness is view of prior art references is no different from that of an infringement analysis. A claim must be construed before determining its validity just as it is first construed before deciding infringement. Only when a claim is properly understood can a determination be made whether the claim ‘reads on’ an accused device or method (patent infringement), or whether the prior art anticipates and/or renders obvious the claimed invention (patent invalidity).

Patent Infringement: [The court extensively analyzed the 1-click process, including the prosecution history of the '411 patent, written description and file history. It concluded that] when the correct meaning of the single action limitation is read on the accused B&N system, it becomes apparent that the limitations of claim 1 are met by the accused [B&N]
system [and thus it is infringing]. After a full review of the record before us, we conclude that under a proper claim interpretation, Amazon has made the showing that it is likely to succeed at trial on its infringement case. Given that ... Amazon has demonstrated likely literal infringement ... we need not consider infringement under the doctrine of equivalents. The question remaining, however, is whether the [trial] court correctly determined that B&N failed to mount a substantial challenge to the validity of the claims in the '411 patent.

*Patent Invalidity:* In an invalidity analysis, the district court must assess the meaning of the prior art references. [The district court found likely infringement by BN, and so it did not focus its analysis on the validity issue.] In this case, we find that the district court committed clear error by misreading the factual content of the prior art references cited by B&N. Each of the [4] asserted references [by B&N] clearly teach key limitations of the claims of the patent in suit. One of the references ... the ‘CompuServe Trend System,’ ... appears to have used ‘single action ordering technology.’ [Also] B&Ns expert, Dr. Lockwood testified that he developed an on-line ordering system called ‘Web Basket,’ an embodiment of a ‘shopping cart ordering component,’ [because of its] ‘cookie specifications.’ [Also] an excerpt from a book ... [explains how to] modify shopping cart ordering software to skip unnecessary steps. [Finally] a web page describing the ‘Oliver’s Market’ ordering system [features this line]: ‘A single click on its picture is all it takes to order an item.’

**Conclusion**

While it appears ... that Amazon has carried its burden with respect to demonstrating the likelihood of success on infringement, it is also true that B&N has raised substantial questions as to validity of the '411 patent. For that reason, we must conclude that the necessary prerequisites for entry of a preliminary injunction are presently lacking. We therefore vacate the preliminary injunction.

**Case Questions**

1. What observations do you have about Amazon's strategy of what is, in essence, a preemptive strike in court to establish its patent rights?
2. What business decisions should Amazon make immediately following this decision?
3. How may B&N modify its online order system following this decision?

Amazon and B&N eventually settled out of court. The terms of the parties' settlement are confidential, with Amazon reportedly pleased to put this matter behind it, and Jeff Bezos reportedly suggesting a shorter term for BMPs, rather than the standard twenty years for other classes of patents [Nick Wingfield, “Amazon, Barnes & Noble.com Settle Long-Lasting Technology Patent Suit,” *Wall Street Journal* (March 6, 2002), p. 1].

**The Doctrine of Equivalents**

This second theory of patent infringement was judicially created by the Supreme Court 150 years ago, in *Winans v. Denmead*, 15 How. 330, 347 (1854). The *doctrine of*
equivalents is a rule that competitors cannot simply make insignificant changes to a patented object to avoid infringement claims. This rule takes the incentive away from reverse engineering and making minor changes so as to avoid literal infringement charges. It further extends the reach of patent claims to prevent "copycats" from reaping benefits from the patented inventions of others. This policy grants patent holders a right to control inventions beyond even those claims covered in the patent. Thus doctrine of equivalents permits a finding of patent infringement, even when the claims are not literally infringed.

The Supreme Court decided a challenge to the doctrine of equivalents in the case Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co., Ltd, 122 S. Ct. 1831, 2002 U.S. LEXIS 3818 (May 28, 2002). The Supreme Court unanimously upheld this doctrine and ruled that it is up to the patent holder to prove the doctrine of equivalents applies against copycats. This decision affirms the worth of existing patents in that it encourages competitors to invest in their own innovative products, rather than attempt to copy existing products.

**Defendant’s Case**

Filing a patent infringement case, even with the presumption in plaintiff’s favor, does not mean automatic liability for defendants. There are a number of theories under which defendants may escape liability. Defendants may be able to challenge the patent itself, with proof that it is invalid, that the listed inventors are not the real inventors, and so forth. These defenses are as follows.

**Noninfringement**

Defendants must prove their process is not the same, in every way, as plaintiff’s process—that it is qualitatively different from plaintiff’s and not a copycat. In one case, ACTV, Inc. v. Walt Disney Co., 2002 U.S. Dist. LEXIS 9267 (May 24, 2002), a federal court considered a noninfringement defense that defendant raised. Plaintiff patented a system for synchronizing Internet programming drawn from sites throughout the Web—with video and television programming. Defendants’ system offers subscribers the ability to synchronize certain Disney television programs with certain Disney Web sites. The court agreed with Disney and found noninfringement because the accused device (Disney’s) did not meet every limitation of plaintiff’s patent, either literally or by equivalents.

**Invalidity**

Defendants must prove that one of the conditions for patentability was not met by the plaintiffs in the first place. For example, the USPTO should never have issued a patent to plaintiff, because plaintiff’s process was not new, or useful, or nonobvious. This could be due to the existence of prior art (defendants publicly used that process for one year prior), or that plaintiff’s process was easily anticipated, or that it did not produce a useful result. There is a strong presumption of patent validity—as to each claim. This means defendant’s burden of establishing invalidity is very difficult to
prove because invalidity must be shown by "clear and convincing evidence." Patent invalidity is the main assertion behind Justice Stevens's dissent and the rationale of those who object to the concept of business methods patents.

The Federal Circuit recently heard a public use case. In Netscape Communications Corp. v. Microsoft Corp., 2002 U.S. App. LEXIS 13840 (Fed. Cir. July 9, 2002), the court reviewed patents that allow computer users to access and search a database residing on a remote computer. The developer gave demonstrations to others of prototypes of his invention at his laboratory. The court considered whether this was a public use that would negate anyone else's patent for this process. The court noted that inventors may test their inventions in public without it being a public use, and it would look to see whether any confidentiality provisions were made and how ready the process was for patenting.

**Remedies**

Patent infringement law is civil and there are no criminal provisions, as there are for the other three types of intellectual property. Plaintiffs are limited to the remedies described here. The statute of limitations for filing a patent infringement suit is six years.

1. **Equitable remedies** This is the most important of the remedies. Courts have the power to assign patents, rewrite inventorship, and prevent violations of any rights secured by the patent.

2. **Damages** Successful plaintiffs are entitled to at least the amount of what a reasonable royalty would have been, plus interest and costs, and any lost profits, if they can be proven. Court may increase by three times this amount for cases of willful infringement.

3. **Attorney's fees** Successful plaintiffs are entitled, in exceptional cases, to reasonable attorney fees.

**THE FUTURE OF BUSINESS METHODS PATENTS: THE PROBLEMS/VULNERABILITIES IN THE PRESENT SYSTEM**

**Prior Art**

The collection of prior art for tangible assets is a great deal easier than collecting the same for intangible assets such as software. Moreover, whereas prior art has been collected for all classes of patents since the issuance of Patent No. 1, no prior art was collected on software or business methods prior to the *State Street Bank & Trust* decision. There has been no discussion of retroactively collecting and cataloging prior art for business method patents either, and that begs the question of how good these patents are. You need only refer back to the *Amazon* case to know the answer.
Additionally, although Rule 56 of the Patent Code requires patent applicants to supply all relevant prior art that is “known” to them, it does not require applicants to search actively for prior art that could invalidate their own applications. This has a sort of ostrich effect.

**Valuation Issues**

This question relates to how much business methods patents are worth. Intangible assets are by definition harder to value than tangible assets. This rush to patent every conceivable process is driven in part by business efforts to create value/shareholder wealth. Potential and actual investors rely on this information, yet how valuable are these intellectual property assets? And how accurate are the accountants’ estimates? It is a guess at this time. Accounting standards are not yet fully developed in this respect, leading to uncertainty and volatility in those companies that have a relatively large intellectual property portfolio. A second and related question is whether patents create value. This is unclear. There is a perception that the costs of business methods patent protection exceed the benefits. For example, in efforts to create open code projects, developers stall when there is a question whether some business may have a patent that may involve the technology—this is the hold-up phenomenon where business methods patents impinge business development. A secondary effect is that the patents act as a concentrator of economic power, excessively enriching those who were first to file at the Patent Office.

**Lock-Up on Information**

The Internet was designed as an open platform: it is the ultimate open and free communication system. It was built without patents, but patents are being grafted onto the very structure of the Internet (i.e., ordering systems, ad displays, transfer protocols, etc.). When we patent such processes, we are taking away parts of the open and free structure, replacing it with gateways, tollbooths, and worse: we are stifling the very openness that is the Internet’s hallmark.

It is an open question, too, whether these patents on business methods actually “promote the useful arts and sciences,” as the patent system is meant to do. Business methods patents are monopolies on information goods. These are inherently different from tangible goods (for which the patent system is better equipped). Information goods are nonrival goods, meaning there is no rival, no real, perfect substitute for them. This begs the question of why a patent is needed for a good that has no true rival. We are thereby locking up information and not necessarily promoting the useful arts and sciences.

In one lawsuit, for example, British Telecom filed an infringement suit against Prodigy seeking royalty payments for its 1989 U.S. Patent No. 4,873,662 covering hyperlink technology. Do we owe British Telecom a royalty every time we click on a link?
The Patent Office

The PTO is paid by the number of patents it issues. Clearly an alternative fee structure needs to be established. There needs to be other incentives for the USPTO to generate quality work. This is under study, per the American Inventors Protection Act. They are now encouraging consistency, focus on finding the invention and searching strategies, and developing a mandatory search scope. Examiner training in substantive patent areas, such as advanced networking, financial transactions, smart cards, accounting, and insurance will add a second-level review before allowance of patent.

INTERNATIONAL RECOGNITION AND ENFORCEMENT OF BUSINESS METHODS PATENTS

Patent Cooperation Treaty

International protection for patents is essential in a global information economy. Recognizing the need to harmonize laws, as well as centralize the administration of patents, the World Intellectual Property Organization (WIPO) plays a central role in these efforts. Before this centralization, it was necessary for patent holders to prosecute and register their patents in every country they wished to conduct business in and comply with as many laws and regulations.

The Patent Cooperation Treaty (PCT) simplifies and reduces the costs of obtaining international patent protection and facilitates public access to a wealth of technical information relating to inventions. By filing one international patent application under the PCT, inventors can simultaneously gain protection in over a hundred nations. (See the WIPO site mentioned earlier.) Inventors would first file their patent application with the PTO and also file an international application with the PTO, which acts as a receiving office for WIPO. Unfortunately, Europe’s interpretation of the PCT has been less than friendly to business methods patents. In February 2002, the European Patent Office (EPO), an organization formed to establish a uniform patent system in Europe, announced it will not function as a searching authority under the PCT for business methods patents filed by U.S. nationals. Although business methods patents are now recognized in the United States their status globally is far from clear. A number of nations and international organizations are struggling with the issue of whether to recognize business methods patents. Surprisingly, very few other nations have followed the U.S. lead in fully recognizing business methods patents.

European Union (EU)

The European Union (EU), through the European Patent Office (EPO), complies with the European Patent Convention. There appears to be only a limited amount of oppor-
opportunities to secure business process patents in Europe. The EU treats business methods in two classes—those that contain technical features and those that do not. Business methods that possess both technical and nontechnical components may be patentable if the technical feature provides a sufficient patentable contribution. Therefore, U.S. patent filers of business processes must ensure that any European application contains a sufficient technical contribution.

In 2000, the EU Directorate General for the Internal Market published a paper on the patentability of computer-implemented inventions. It represents an attempt to reconcile the exclusion of the patentability of computer programs with the reality of thousands of patented technical inventions found in computer programs. They concluded that a computer-implemented invention which merely automates a known process does not involve an inventive step.

World Intellectual Property Organization (WIPO)

WIPO is an international organization dedicating to the promotion of human creativity and the protection of intellectual property. In WIPO's “Primer on Electronic Commerce and Intellectual Property Issues,” WIPO recognizes that patents have been increasingly granted in the United States for financial services, Internet advertising, and e-commerce billing methods. However, WIPO recognizes that commentators have criticized e-commerce business methods patents because they do not reflect new ways of doing business and the only aspect different from traditional business methods is that they occur in cyberspace.

Japan

In November 2000, the Japanese Patent Office (JPO) published a draft document titled, “Policies Concerning ‘Business Methods Patents.’” The policy was motivated in part by advancements of Internet-related technology and provides that “as personal computers and the Internet become popular, ‘business method-related inventions’ utilizing known computers and communication technology come to attract attention from service industries, financial or advertising etc., which have not formerly been interested in the Patent System.” Japanese patent law recognizes patents only for inventions that have industrial applicability and exploit the laws of nature.

In January 2001, the JPO published final guidelines that focus on the patentability of software-related inventions. The JPO currently requires that inventions have a “statutory invention” and an “inventive step.” The statutory invention prong requires “a creation of technical ideas using the law of nature.” The inventive step requires in essence that the patent not be obvious to someone versed in the field. These steps allow for the filing and approval of business methods patents, but are limited to software-related applications. Because many Internet-related business methods
patents involve software, the patentability of such methods in Japan may soon equal the breadth under U.S. law.

**Extraterritorial Enforcement of Business Methods Patents**

The differing view of the validity of business methods patents worldwide presents significant obstacles for U.S. businesses. Applicants for business methods patents must consider both the current and future trends in international patent law when deciding on a strategy to pursue. Limited opportunities exist to protect American holders of business methods patents outside the United States.

The most obvious choice for enforcing business methods patents is to bring suit in the United States against the infringing party. Section 402(1)(c) of the Restatement of Foreign Relations provides that a country has "jurisdiction to prescribe law with respect to . . . conduct outside its territory that has or has intended to have a substantial effect within its territory." However, U.S. courts would apply the law only if that foreign state’s law recognizes the patentability of business methods.

Another provision, section 271(g) of the Patent Act of 1994, allows businesses to block the importation of infringing products into the United States. The patent holder must show a connection between the alleged infringement and the imported product. If the product is a direct result of a violation of the patent, the patentee may block the importation of that product. However, to invoke this law, it must be shown the patent was an essential part of the development or manufacturing process. In most situations, infringers can escape persecution because alternative methods of production exist.

**Trade Secrets: An Alternative Strategy to Patenting**

**Legal Framework of Trade Secrets**

A trade secret is secret information owned or developed by a business that gives it a competitive advantage. The laws relating to trade secrets were developed by judges at common law, in order to provide a remedy for businesses that suffer economic damages related to the improper disclosure or theft of proprietary secrets to competitors. These laws were originally based on theories related to breach of fiduciary duty or breach of contract. A series of statutes have been enacted, and so there are a variety of state and federal remedies to pursue for such injuries.

Trade secret protection is an alternative to patent protection, and it may accomplish the same goals, and more. Trade secret protection is not secured with the grant of a government-sponsored monopoly, as is the case with copyrights and patents. Rather, trade secret protection is developed with no government intervention at all (this is similar to trademarks where rights arise from use rather than registration). Trade secret protection is accomplished through proprietary efforts by the business to develop and then continually maintain the secret. The scope of subject matter that may be treated as a trade secret differs as well. Trade secret protection covers potentially anything of economic value to a business, and so coverage is greater than say, for example, patents, where the subject matter must be novel, useful, and nonobvious.
For example, although customer lists or invoices do not qualify as patentable subject matter, they clearly have economic value and may be protected as trade secrets. The Patent Office demands that all relevant information for patents be publicly disclosed, but a trade secret is just that—secret and potentially never available to the public. Finally, whereas patents have a limited lifetime, trade secrets have a potentially unlimited lifetime, protected as long as the company engages in continuous efforts at confidentiality.

**Trade Secret Laws.** Trade secret laws are enforced by a patchwork of federal and state laws. First, there is the Economic Espionage Act. Subtle differences exist in the laws, but trade secret laws have three elements in common. A trade secret (1) is known only to the business; (2) it affords the business a competitive advantage over others in its industry; and (3) is kept secret continuously by means of reasonable steps. Owners of trade secrets can enforce rights against those who disclose, misappropriate, or steal the secrets, but most significantly, they cannot enforce rights against those who independently develop or reverse-engineer the secrets.

**Economic Espionage Act (EEA)** This is the federal act addressing trade secrets. More about this statute appears in Chapter 12. According to the EEA,

‘Trade Secret’ means all forms and types of financial, business, scientific, technical ... information, whether tangible or intangible ... if:

(A) the owner thereof has taken reasonable measures to keep such information secret; and

(B) the information derives the independent economic value ... from not being generally known ... and not being readily ascertainable through proper means by, the public ... .

**Uniform Trade Secrets Act (UTSA)** The language of the Uniform Trade Secrets Act is virtually identical to the Economic Espionage Act in its definition of a trade secret. This model law has been adopted by approximately forty-one states.

**State Laws** Because the Uniform Act has not been adopted by every state, it is important to consult the law of the forum state. (This inevitably leads to forum shopping.) We cite the California trade secret law here because California is frequently a forum for litigation in this area, and in fact it is handling the DVD Copyright Control Association case.

California Civil Code section 3426, Uniform Trade Secrets Act (in part) states,

‘Trade Secret’ means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and

http:// To read the Economic Espionage Act, see http://www4.law.cornell.edu/uscode/18/plch90.html

http:// To read the Uniform Trade Secrets Act, adopted by a number of states, see http://nsi.org/Library/Espionage/usta.htm
Part 2 Intellectual Property Issues in Cyberspace

(2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Trade Secret Law as It Relates to Business Practices

Trade Secret Subject Matter. A trade secret may encompass more and different types of information than would be patentable and may include general information, procedures, billing, account information, lists/compilations, formulae, patterns, program devices, methods, techniques, processes, strategies, marketing plans, and pricing information.

Some example of trade secrets are Colonel Sanders’s secret recipe, McDonald’s special sauce, Smith’s Black Cough Drops, Kodak, and the Coca-Cola formula. (The Listerine formula was initially protected by a trade secret until its formula was published in a journal.)

Maintaining Trade Secrets. The most difficult part of controlling trade secrets is maintaining it as a secret. The standard for information to be considered a trade secret is that it must be the subject of continuous efforts that are reasonable under the circumstances to maintain its secrecy. Businesses must formulate a strategy that controls all points where trade secrets might be leaked: the network, employees, or others who have a working relationship with the business.

Employee Duties. Employees have a fiduciary duty to their employers not to disclose company secrets.

As more trade secrets are in digital format, they are ever easier to steal, misappropriate, or publish on the Internet. It is a critical management task to control employee access, knowledge, and use of trade secrets.

Trade Secret Agreements. Strategies to protect trade secrets, therefore, take on a heightened importance. To accomplish this goal, businesses often require employees and others with insider knowledge (such as vendors, suppliers, partners, and clients) to sign nondisclosure agreements, noncompetition agreements, and/or nonsolicitation agreements.

Nondisclosure agreements prohibit parties from disclosing confidential information. Defining what is, and is not, confidential information is crucial. Such agreements should also cover acceptable (and unacceptable) uses of the information, as well as the duration of the agreement. These agreements are appropriate for employees, officers, directors, vendors, suppliers, partners, clients, and even bankers, lawyers, and accountants who are privy to quite a bit of insider information.

Noncompetition agreements prohibit parties from competing with the business for a period of time and within a certain geographic area. These agreements are appropriate for employees and officers of the business. Noncompetition agreements are generally enforceable if they protect a legitimate business interest and are reasonable in scope, duration, and geographic limitation. Significantly, California does not
recognize noncompetition agreements. In one recent case, eBay (based in California) and Amazon (based in Washington) were in litigation over an executive who left Amazon to go to eBay, and one of the most contested points was where the suit should be heard—because the location is dispositive in many of these cases.)

Finally, businesses use **nonsolicitation agreements** that prohibit parties from attempting to lure away employees who may have knowledge or access to trade secrets. These agreements are appropriate for the business’s partners. Note how these agreements, which are used for important and legitimate reasons, negatively impact job mobility and opportunities for employees.

*Maintaining Physical and Network Security* Where it is possible to have trade secrets in digital format, it becomes an easy endeavor to steal them and then post them on the Internet, so they lose their status as a trade secret—and never get caught because the perpetrators did this anonymously. Controlling access to the secrets, and locking them up, for example in an encrypted file, is an almost necessary strategy in establishing that the trade secrets were the subject of continuous reasonable efforts to maintain their secrecy. The actual securing of trade secrets is an issue that deserves more attention from businesses. (Refer also to Chapter 11 on this issue.)

*How Trade Secrets Rights Are Lost.* Trade secrets can be lost in a number of ways: when the secret is reverse-engineered, independently developed, or published, or when the business fails to continuously maintain secrecy. Note how with respect to these occurrences that although the trade secret protection is lost, had these secrets been patented, the patent protection would have continued, in spite of these negative events.

*Trade Secret Litigation: Plaintiff’s Case*

Plaintiffs must prove the elements of the statutes they are filing suit under. For example, they must show the existence and ownership of a trade secret that derives independent value from not being generally known and they have continuously maintained. They will need to prove that defendants had access to the trade secrets; that they had notice the information was protected as a trade secret (this could be accomplished by use of the agreements mentioned); and that defendants used the trade secrets. Then plaintiffs allege any of the following causes of action. (Note that in many of the corporate defamation/cybersmear lawsuits that the posters are, in most instances, publishing trade secrets. (Refer to Chapter 11, “Defamation.”)

**Misappropriation.** It is illegal to misappropriate or use improper means to acquire a trade secret. A claim is made when the following exists:

- Ownership of a trade secret; and
- Theft, bribery, misrepresentation, breach, or inducement of a breach of a duty to maintain secrecy or espionage through electronic or other means; or
- **Misappropriation** (the acquisition of a trade secret by one who knows or has reason to know the trade secret was acquired by improper means or wrongful disclosure of a trade secret to another without consent).
**Breach of Contract.** Breach of contract claims usually are due to a breach of the employment agreement, specifically the noncompetition, nondisclosure, or nonsolicitation clauses. These agreements generally create a legal duty not to disclose the trade secrets without permission.

**Inevitable Disclosure.** The claim of inevitable disclosure is used when the former employee had access to inside information and trade secrets, thereby possessing extensive and intimate knowledge about company operations and strategy. The business may sue to prevent the former employee from going to work for a competitor under the inevitable disclosure doctrine, which holds that the employee would inevitably disclose the trade secrets of his or her former employer and so may not be trusted to protect the former employer’s trade secrets. This theory effectively presumes that employees are going to do something wrong; the theory works best when the former and new business share or potentially share many of the same customers and markets. For a case on this doctrine, see *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262 (7th Cir. 1995) (the former Pepsi employee was not allowed to assume his duties with Quaker, where he was to oversee the Gatorade and Snapple brands).

**Trade Secret Litigation Continued: Defendant’s Case**

To be successful, defendants have to disprove any of plaintiff’s proofs. For example, defendants would have to show the information was not a protected trade secret (due to disclosure, inadequate protections, etc.) or that defendants did not have access to the trade secret, or notice it was a trade secret, or did not use the trade secret.

**Public Disclosure/Publication of the Trade Secret.** A trade secret cannot be a secret if the contents of it have been disclosed. So defendants would have to prove a publication of the secret, which is relatively easy to do. In terra firma, public disclosure occurs when the trade secret is published in print form or becomes well known throughout that industry. In cyberspace, however, public disclosure is a matter of a few clicks; it occurs when the trade secret is published anywhere on the Internet. In fact, there are instances of anonymous publishers (usually disgruntled present or former employees) of trade secrets on the Internet. The trade secret loses its status as a trade secret, and the posters of the trade secret are in a sense judgment proof because they cannot be found.

Consider this important and recent disclosure case:

**DVD Copy Control Association v. Bunner**

*93 Cal. App. 4th 648, 2001 Cal. App. LEXIS 1179 (November 1, 2001)*

This decision was withdrawn, however, because the California Supreme Court granted a petition for review: 41 P.3d 2, 2002 Cal. LEXIS 614 (February 20, 2002). This case is still pending.
Facts

The DVD Copy Control Association (the Association) is an industry-sponsored not-for-profit group responsible for licensing the Digital Versatile Disk (DVD) industry’s Content Scrambling System, known as CSS. CSS is an encryption system and designed so DVDs may be played only on CSS-equipped players or drives. (It also—to some extent—prevents unauthorized use.) The typical licensees are manufacturers of stand-alone DVD players and DVD drives installed in computers that run Windows operating systems. No DVD players or drives were licensed for computers running alternative operating systems such as Linux. In October 1999, a fifteen-year-old Norwegian boy, Jon Johansen, reverse-engineered the CSS, thereby making it possible to play an encrypted DVD on a non-CSS-equipped DVD player or drive. He named this program DeCSS. The first posting of DeCSS appeared in October 1999, and soon thereafter it appeared on a number of sites worldwide. Andrew Bunner republished the DeCSS program. (Other individuals posted only links to the DeCSS program, without actually republishing the DeCSS.) The Association filed suit in late December 1999 against more than fifty Web site operators who allegedly posted information about DeCSS on their sites.

The Association initiated an action under the UTSA, charging that the master codes in the CSS and, consequently, the DeCSS are protected trade secrets. The Association is suing Bunner and others in order to suppress their dissemination of DeCSS over the Internet. The Association alleges that it protected this proprietary information by (1) limiting its disclosure to those who had signed licensing agreements, and (2) prohibiting disclosure to all others. The license agreement states that the CSS is a confidential trade secret. It is unclear in the pleadings whether the Association’s licensing agreements, or other user agreements (click-wrap, browse-wrap, etc.) contained any clause prohibiting the act of reverse-engineering CSS. DVD CCA requested equitable relief in the form of a temporary restraining order and a preliminary injunction. The state trial court agreed with the Association and ordered Bunner and others to refrain from republishing DeCSS. The state appeals court reversed this order for a preliminary injunction, concluding it amounted to an impermissible prior restraint on speech in violation of Bunner’s First Amendment rights.

What are the issues on appeal and how should they be resolved?

The Association’s Arguments

• It has a trade secret (valuable information and reasonable efforts to keep it a secret.
• Bunner’s actions violated the UTSA because DeCSS discloses the trade secret master keys; the master key was obtained by improper means; and Bunner had reason to know this.
• DeCSS was substantially derived from proprietary information property or trade secrets of the CSS.
• The applicable law is California law, not the law of Norway, and the Association need only show that improper means were used to gain the information.
• The Association concedes that computer code is speech, but argues it is entitled to relief because it would suffer severe and irreparable harm.
• The Association suggests it has a License Agreement that restricts reverse engineering (but it is unclear whether their licensing agreements are explicit on this point).
Bunner’s Arguments

- Posting of DeCSS, or any code, for that matter is an expressive right protected by the First Amendment, and the government may not burden that right—unless it has a compelling reason to do so, and the means chosen are narrowly tailored to achieve that end.
- There is no evidence that he knew, or should have known, that DeCSS was created by improper use of any proprietary information. He was merely a republisher.
- He was never an employee of the Association and so never breached any agreement about nondisclosure.
- In Norway, for example, reverse engineering of software is permitted for the purpose of achieving interoperability, despite any agreement to the contrary.
- Publication of programs such as DeCSS, decrypting supposedly secure encryption (in this case by a fifteen-year-old) actually serves a very beneficial public interest—by notifying the makers and the public of security flaws in software.
- He saw DeCSS on the slashdot.org site, and merely republished it so other programmers could modify and improve DeCSS—in the way that open-source programmers collaborate to improve programs. He alleges he had no reason to believe it was improperly reverse engineered or misappropriated.
- Finally, he asserted that the repeated postings of this alleged trade secret caused it to become public knowledge anyway, and so the code lost its status as a trade secret.

As improbable as it seems, the Association revealed—in an open court session—the trade secrets it said Bunner improperly released. Realizing its blunder, the Association then requested the court to seal the documents, and the judge obliged.

An important observation in this case that deserves discussion: note how the trial court’s decision impacts Bunner’s rights of speech. This speech issue is more fully developed in Chapter 10, “Obscenity,” and Chapter 13, “Internet and Computer Crime.”

In a recent case, Ingenix filed suit against a former employee. It asked the court for an injunction to prevent the former employee from using or disclosing any of Ingenix’s business, customer, pricing and marketing information, and from soliciting business from any of Ingenix’s clients. The court granted the plaintiff’s request where it found that the information was maintained as a series of trade secrets; that the former employee had access to it and notice of its trade secret status, and that it would be used. The former employee’s e-mails proved this, and so did audit logs of his computer use [Ingenix, Inc. v. Lagalante, 2002 U.S. Dist. LEXIS 5795 (E.D. La. March 28, 2002)].

Reverse Engineering. Reverse engineering is a defense to trade secret misappropriation claims. Although under patent law, it is unlawful infringement to reverse-engineer an
invention, it is not illegal under trade secret law. But most digital products or services contain agreements, such as click-wraps and browse-wraps that prohibit reverse engineering. So, even though plaintiffs could not bring a trade secret misappropriation claim, they may still have available a breach of contract claim for the act of reverse engineering.

**Independent Derivation.** The independent derivation defense arises when the same secret was developed independently by another. Courts must undertake an extremely detailed fact-specific investigation, including dates of development, the state of this knowledge in the industry, and so forth.

**Remedies.** If plaintiffs prove their case, there are a number of applicable remedies:

1. **Injunction** By virtue of a court order, plaintiffs may be able to regain control of the trade secret or stop use of the trade secret.
2. **Damages** Compensatory damages are available. In exceptional cases, punitive damages (up to twice the compensatory damages) as well as attorney fees are available.
3. **Imprisonment** Criminal penalties are invoked for cases of trade secret theft. (Refer to Chapter 12.)

**International Recognition and Enforcement of Trade Secret Laws**

**Global Recognition of Trade Secret Laws.** Unlike business methods patents, trade secrets have received significant international recognition and protection for some time. For example, the Paris Convention prohibits unfair trade practices among its members. The Paris Convention states that unfair trade practices include "[a]ny act of competition which is in conflict with the fair customs of industry and trade." Although examples provided by the Paris Convention do not explicitly include trade secrets, trade secret infringement could likely be interpreted as a form of "unfair competition" under its provisions.

**Trade-Related Aspects of Intellectual Property Rights (TRIPS).** TRIPS is a widely recognized international agreement that reaffirms earlier intellectual property treaties such as the Paris Convention and requires signatories to afford equal intellectual property treatment to nationals of signatory nations. TRIPS also requires nations to develop laws to protect intellectual property, establish dispute settlement procedures, and enforce these intellectual property rights.

The most relevant TRIPS provision to trade secret protection is Article 39(2), which states,

Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices so long as such information:

(a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to
persons within the circles that normally deal with the kind of information in question;

(b) has commercial value because it is secret; and

(c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

Although this section does not use the phrase “trade secret,” it clearly contemplates protection for undisclosed commercial information. Article 39(2) requires that the information must be secret and not generally known among individuals knowledgeable in the field. Also, the information must have some commercial value in the marketplace. Finally, the owners of the information must have taken some steps to keep the information from public disclosure.

The phrase “manner contrary to honest commercial practices” arguably encompasses a broad range of improper disclosures such as breach of confidence by a confidant and the acquisition of the information by third parties who knew or should have known the practice in question was a trade secret. Thus the violation of trade secrets under TRIPS may include unlawful disclosers as well as third-party acquirers of secret information.

**North American Free Trade Agreement (NAFTA).** NAFTA, an agreement that regulates trade between the United States, Canada, and Mexico, contains a section that establishes uniform minimum trade secret standards. Article 1711(1) states,

> Each Party shall provide the legal means for any person to prevent trade secrets from being disclosed to, acquired by, or used by others without the consent of the person lawfully in control of the information in a manner contrary to honest commercial practices, in so far as:

- To examine the NAFTA treaty further, see [http://www.nafta-secalena.org](http://www.nafta-secalena.org)

(a) the information is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons that normally deal with the kind of information in question;

(b) the information has actual or potential commercial value because it is secret; and

(c) the person lawfully in control of the information has taken reasonable steps under the circumstances to keep it secret.

NAFTA protection practically mirrors the protection provided by TRIPS. However, some differences do exist. For example, NAFTA more broadly defines sufficient value as having “actual or potential commercial value.” TRIPS does not make this distinction. In addition, Article 1711(3) and (4) prohibits NAFTA members from placing any limits on the duration of trade secret protection. TRIPS does not similarly discuss duration of trade secrets.
**Global Enforcement of Trade Secret Laws.** A company trying to protect its trade secrets may be required to bring the violator to court. The company has two choices: sue the discloser in the United States, or in the foreign country where the violations occurred.

**Enforcing Trade Secret Protection in an International or Foreign Forum** Traditionally, legal actions for trade secret violations in another country would have to be pursued in that country. This leaves U.S. companies at the mercy of different, and potentially lax, trade secret protections in that nation.

TRIPS attempts to solve this problem. TRIPS requires members to establish national enforcement systems that resolve intellectual property violations. Article 63 requires that any law, regulation, administrative ruling, or court decision related to TRIPS must be available for public examination. A TRIPS council exists to monitor compliance with this and other provisions. The enforcement provisions of TRIPS (Articles 41–47) require members to establish evidence production requirements and permit remedies such as injunctions and compensatory damages. Any TRIPS member should have viable enforcement and judicial mechanisms in place for extraterritorial protection of trade secrets. If the company holds a valid judgment in the United States, that judgment is recognized in other member countries as binding.

**Enforcing Foreign Trade Secret Judgments in the United States** A trade secret judgment in a foreign country may influence the decision of a U.S. court. Although case law is unsettled on this point, some legal principles seem clear. A majority of states have enacted the Uniform Foreign Money-Judgments Recognition Act, providing that foreign judgments are generally recognizable, with exceptions, including for fraud, repugnance to public policy, or conflict with another judgment.

**Summary**

Business methods patents and trade secrets protection represent additional important and useful methods for managing intellectual property assets. Patenting business methods is a key strategy in the new economy, both as a way to control product and service development upstream and to license or assign rights downstream. It remains to be seen whether business methods patents can withstand the present criticism and scrutiny of their worth and economic value. Protecting assets by way of trade secrets offers greater flexibility and a potentially unlimited life span, but at the cost of making a diligent, concerted, and continuous effort to protect those secrets. Both of these methods offer legal protections, and they should be considered as complementary for businesses making decisions on intellectual property asset protection and control. Business methods patents and trade secrets must also be protected on a global level. Although most patents are recognized internationally, business methods patents receive limited or no protection in many nations. Similarly, trade secrets may not be recognized in countries without developed trade secret laws.
Key Terms

- patent, 112
- U.S. Patent & Trademark Office (USPTO), 113
- Patent Act, 113
- American Inventors Protection Act, 114
- prior art, 115
- business methods patents, 119
- infringement, 126
- doctrine of equivalents, 128
- World Intellectual Property Organization (WIPO), 132
- Patent Cooperation Treaty (PCT), 132
- European Union (EU), 132
- trade secret, 134
- Economic Espionage Act, 135
- Uniform Trade Secrets Act, 135
- nondisclosure agreements, 136
- noncompetition agreements, 136
- nonsolicitation agreements, 137
- misappropriation, 137
- inevitable disclosure, 138
- reverse engineering, 140
- independent derivation, 141
- Paris Convention, 141
- Trade-Related Aspects of Intellectual Property Rights (TRIPS), 141
- North American Free Trade Agreement (NAFTA), 142
- Uniform Foreign Money Judgments Recognition Act, 143

Manager's Checklist

- Patent law is a specialized area, and any discussion of patent strategies and procedures should take place with legal counsel.
- Software has expressive as well as functional components and may be proper subject matter for copyright and/or patent protection.
- Patents have many uses, and a comprehensive strategy should be considered to maximize these assets.
- In deciding whether to protect information as a patent or a trade secret, consider the many features of each method, and, again, consult legal counsel.
- With regard to the risks associated with trade secrets, the major security vulnerability is with those most closely associated with the company: employees, consultants, vendors, suppliers, clients, and consultants. Manage the risk accordingly.
- Consider agreements with each of these groups so as to control information, use, and disclosure.
- Be aware that business methods patent protection varies widely among countries. For example, they are least protected in Europe, somewhat protected in Japan, and fully recognized in the United States.
- Investigate carefully any foreign company you share trade secret information with. A specific contract should be drafted to regulate control of any trade secrets disclosed.
- Structure your business relationship so there is motivation to preserve your company’s trade secrets. If it is profitable for the foreign company to keep the secret confidential, then it will be more likely that it remains so.
Ethical Considerations

- Companies should make clear policies for ownership of patentable subject matter that employees invent on company time.

- Companies should consider defensive strategies to competitors' patent applications.

- When an inventor offers a company the opportunity to purchase and develop patentable subject matter or a trade secret at the company, the company must consider its obligations to the inventor and how to properly recognize the inventor.

- Companies should consider the use of restrictive agreements, such as non-compete or disclosure clauses, but also be aware of the impact on employees' job mobility.

Case Problems

1. Telular filed a patent infringement suit against Vox2. For pretrial discovery, Telular wants its expert to have access to Vox2 documents. Vox2 objects because these documents are trade secrets. What is the result? [Telular Corp. v. Vox2, Inc., 2001 U.S. Dist. LEXIS 7472 (June 4, 2001)]

2. Mr. Antonious is the owner of U.S. Patent No. 5,482,279 ("the 279 patent"), which is directed to an improved perimeter weighting structure for metal golf club heads. Spalding sells the Intimidator golf club line. The Intimidator line includes drivers and fairway woods that use what Spalding refers to as "titanium insert technology." Antonious saw several Spalding Intimidator metal wood-type golf clubs in retail stores. He purchased one of the Intimidator drivers and cut open the club head. After inspecting the interior of the club head, Antonious concluded that Spalding's club infringed his 279 patent. What are Antonious's legal options? [Antonious v. Spaulding and Evenflo Co., 275 F.3d 1066 (Fed.Cir. 2002)]


4. Plaintiffs read a case study in business school about X-IT. The study contained a lot of detailed information about the company including its customers. X-IT
manufactures and sells mesh rope-style emergency escape ladders, both in stores and through its Web site. After school, plaintiffs bought X-IT and subsequently entered into discussions with Kidde Portable Equipment about a potential deal with X-IT; pursuant to this the parties signed a confidentiality agreement about the negotiations. X-IT’s customer account lists (which included Home Depot) were shown to Kidde during these negotiations. X-IT alleges that a Kidde representative told Home Depot that X-IT was in negotiations to be sold to Kidde. X-IT lost business because of this. X-IT alleges that the list was a trade secret and was misappropriated. What is the result? [X-IT Products, LLC v. Walter Kidde Portable Equipment, Inc., 155 F. Supp.2d 577 (E.D. Va. 2001)] (This is a helpful case detailing a start-up business.)

5. Pepsi-Cola Bottling seeks an order compelling Kansas Vending to produce all records, invoices, purchase orders, and so on, from any transactions with Sam’s Club or any other wholesale merchandiser, for any of Pepsi’s products. Kansas Vending objected to the subpoena order, on the grounds that these documents are trade secrets. What is the result? [Pepsi-Cola Bottling Co. v. PEPSICO, Inc., 2001 U.S. Dist. LEXIS 20153 (D. Kan. November 28, 2001)]

6. The Church of Scientology sued a former member for copyright infringement and trade secret misappropriation for allegedly copying a few church documents and posting them on the Internet. These documents were publicly available due to an earlier court action. What is the copyright result? What is the trade secret result? [Religious Technology Center v. F.A.C.T.Net, Inc., 901 F. Supp. 1519 (D. Col. 1995)]

7. A medical foundation used IDX’s medical billing software. IDX’s competitor is Epic. Two Epic employees left and went to work directly for the medical foundation, and soon thereafter, the foundation switched its software supplier—to Epic. IDX alleges that these two employees used their new positions to transfer valuable information to Epic, about how IDX software works, and so on, thus enabling Epic to enhance its own software package. IDX filed suit alleging the two employees misappropriated IDX’s trade secrets. What is the result? [IDX Systems Corp. v. Epic Systems Corp., 285 F.3d 581 (7th Cir. 2002)]

8. Ford Motor Company filed suit requesting an order barring the operator of a Web site, Robert Lane, who was not a company employee, from posting confidential company documents containing information about its future plans and product plans. Ford alleges that posting these documents disclosed its trade secrets. What is the result? [Ford Motor Co. v. Lane, 67 F. Supp. 2d 745 (E.D. Mich. 1998)]

9. E. Circuit Sales hired Randall and he signed an employment agreement that contained both nondisclosure (of trade secrets or confidential information) and noncompetition clauses. N.E. later filed suit against Randall in an effort to
enforce the employment agreement, after he resigned to go work for a direct competitor of N.E. Circuit Sales. What is the result? [New England Circuit Sales, Inc. v. Randall, 1996 U.S. Dist. 9748 (D. Mass. 1996)]


Additional Readings


Privacy

Recent Inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls (Cooley on Torts, 2nd edition) the right "to be let alone."


LEARNING OBJECTIVES

After you have read this chapter you should be able to:

1. Understand federal and state constitutional sources of the right to privacy.
2. Discuss the four common law torts for invasion of the right to privacy.
3. Discuss the privacy issues and laws related to the collection and disclosure of financial- and health-related personal information.
5. Explore the privacy issues surrounding spamming and online profiling with emphasis on the Federal Trade Commission's efforts to enforce its regulations in this area.
6. Explore workplace privacy issues, in particular, the monitoring of employee computer use and electronic mail (e-mail).
8. Understand the U.S./EU safe harbor rules and how U.S. firms may satisfy them.
9. Comprehend other international initiatives to regulate online privacy.

INTRODUCTION

At the time Warren and Brandeis talked about the concept of a "right to privacy," none had been recognized constitutionally or otherwise. They fervently believed in and advocated that right, and they were also prophetic. When they referred to "recent inventions and business methods," one wonders if they could have foreseen the time when that right to be let alone would be increasingly threatened by global positioning systems that allow auto rental agencies to track the speed and direction of its customers, the FBI's use of advanced technology such as thermal global imaging to pen-
etrate the walls of a house to determine if marijuana was growing inside (see *Kyllo v. U.S.*, 121 S. Ct. 2038, 2001 presented in Chapter 12), surveillance cameras in public places to monitor our activities, employers monitoring employees’ computer usage in the workplace, parents not being able to adequately prevent online Web sites from collecting personal information about their children without permission or notice, or a federal law passed as a result of the most tragic and fearsome foreign threat to the security of our homeland in our history that provides new search and seizure powers to the government in order to assist its efforts to combat and protect us against acts of terrorism. All these no doubt would have made Brandeis and Warren’s “top ten” list of major threats to our privacy.

In this chapter we discuss the evolution of the right to privacy and its application to cyberspace. We also explore important cyberspace privacy considerations precipitated by the privacy laws related to the use of the Internet with major emphasis on the workplace.

The enormous growth of the Internet, not only as a means by which we communicate electronically with one another via e-mail but also a marketing tool for e-businesses, continues to present major privacy issues and concerns. For example, every time we visit a Web site, we leave a kind of footprint containing personal demographic information. To gather this information, businesses use computer files called *cookies* capable of tracking our visits to sites and depositing facts about us on our hard drives. What is bothersome, and has the potential for legal and ethical problems, is the use of this private information for commercial purposes without our permission.

Later in this chapter, we discuss some of the uses of this information including spamming (the bulk e-mailing of unsolicited advertisements) and online profiling of personal information (information about users accessed and gathered by Internet advertisers and others). Also later in this chapter, to illustrate the privacy issues raised by these practices, we study one of the most important cases: *In Re DoubleClick Inc.*, *Privacy Litigation*.

You should first be aware that if you searched the Bill of Rights and all twenty-seven amendments to the U.S. Constitution, you would not find an expressed or enumerated right to privacy. Rather, the right to privacy is a penumbral, or implied right, under the U.S. Constitution. The sources of this right require us to consider the Fourth, Fifth, and Ninth Amendments to the U.S. Constitution as applied to the states by the Fourteenth Amendment. Keep in mind, these amendments protect us from unwarranted government intrusions.

### Sources of the Right to Privacy

#### U.S. Constitution

The *Ninth Amendment* provides:

> The enumeration in the constitution of certain rights shall not be construed to deny or disparage others retained by the people.
This amendment was probably the genesis used by the courts and legal scholars including Warren and Brandeis to create a kind of right to privacy. In addition, the Fourth and Fifth Amendments are also sources of the “right to privacy.” The Fourth Amendment provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no Warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

In *Griswold v. Connecticut* (1965), the U.S. Supreme Court declared unconstitutional a state law prohibiting the use of birth control devices and the giving of advice concerning their use. The Court also recognized that the Bill of Rights provided us with what it deemed to be “zones of privacy,” or areas or locations where privacy is expected.

Later cases held that an important element of this right was to establish the existence of a “reasonable expectation of privacy” (discussed later in more detail) in the particular zone of privacy. The following are minimum requirements for establishing a “reasonable expectation of privacy”:

1. A person exhibits an actual expectation of privacy. Consider what you expect when entering an area or location, such as your bedroom, which you desire to be “off limits” to others. Or consider what level of privacy an employee should anticipate with regard to his or her office, desk, file cabinet, or floppy disk.
2. Society recognizes the expectation as reasonable. In addition to your privacy expectation, what do others believe to be your expectation of privacy when you close the door to your bedroom or your office, enter a public phone booth, send an e-mail, or surf a Web site?

For purposes of our discussion of establishing privacy rights associated with cyberspace, these requirements, at a minimum, will have to be satisfied concerning the mass of information, some of a personal nature, being disseminated and accumulated over the Internet.

We next focus on the provision of the Fifth Amendment that protects us from government actions that could result in self-incrimination. That provision reads in part:

No person . . . shall be compelled, in any criminal case, to be a witness against himself.

This does not apply when a person voluntarily turns over documents, records, files, and papers to a law enforcement agency or official. Similarly, the public records of a corporation are not subject to this provision, even if they contain incriminating evidence.

An interesting cyberlaw application of the Fifth Amendment involves the act of encrypting a file that contains possible incriminating information. Encryption involves using encoding methods (using key codes and secured passwords) to block access to certain documents. In *Doe v. United States*, 487 U.S. 201 (1988), the Supreme Court held that an individual could “be forced to surrender a key to a
Part 4
Special Issues in Cyberspace

strongbox containing incriminating documents, but not to reveal the combination to his wall safe . . . by word or deed." This case seems to imply that a law enforcement agency, pursuant to a valid search warrant, could obtain an encrypted file. However, the decision in Doe would likely prevent the agency from forcing a defendant to supply the private key, password, or code that could enable decryption or decoding, thereby allowing access. Doe raises issues regarding employees who store potentially criminal information on their employer’s computers. If the information belongs to the employer and not the employee, it is possible a court would allow the employer to access it and use it not only to fire the employee but also to provide it to law enforcement officials. Of course, this presupposes that if the employee has encrypted the material sought, the company has the ability either through stated company policy or the law to require the employee to allow access.

State Constitutions

In addition to the U.S. Constitution, state constitutions are a source of privacy rights. In general, these rights mirror the amendments mentioned earlier in content and, similarly, apply only to public employees. However, some states afford greater protection to government violations of privacy. States have afforded privacy protection to electronic eavesdropping (wiretapping), medical, insurance, school records, credit and banking information, and so on. You should also recognize that the states, under the common law, grant privacy protection to what are called certain “privileged” communications. For example, with very limited exceptions, what a client tells an attorney or what a patient tells a physician is private and not available to anyone, including government officials, unless voluntarily disclosed by the client or patient.

Attorney-Client Privilege and the Use of E-Mail

A growing privacy concern involves the extensive use of e-mail, via computers and Palm Pilots, by attorneys (in 2000, the American Bar Association estimated 94 percent use it) to communicate with their clients and the possibility of unauthorized access of this information by others, thereby jeopardizing the confidentiality of the communications. Thus far, the issue of e-mail and the attorney-client privilege has yet to be decided by the courts. Attorneys and others (doctors, psychiatrists, etc.) who electronically communicate confidential information to their clients or patients should, at the very least, seek the most effective methods such as encryption to protect them.

http://

- Check your state's government to see what privacy rights are provided under state law from links at http://www.law.cornell.edu/states/listing.html

Common Law Torts for Invasion of Privacy

Our focus next shifts to the four types of torts recognized at common law and by the Restatement (Second) of Torts. These provide monetary and injunctive relief for an unreasonable or unwarranted invasion of the right to privacy. Conceivably, they could also provide remedies for a cause of action in cases involving privacy rights in cyberspace. These torts are Intrusion upon Seclusion; Public Disclosure of Private Facts
Causing Injury to Reputation; Publicly Placing Another in a False Light; and Misappropriation of a Person's Name or Likeness Causing Injury to Reputation.

Intrusion upon Seclusion

On occasion, most of us have wished to enjoy what Judge Cooley recognized as a basic "right to be let alone," to go to a place of seclusion. Of course, like most of our legal rights, this right is not absolute. However, when another individual, without permission or legal justification, violates that place of seclusion, this tort could provide a remedy. The Restatement (Second) of Torts defines Intrusion upon Seclusion as:

Intentionally intruding, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns.

In order to succeed, a plaintiff would have to prove the following elements:

- There was intent to intrude or knowledge that the intrusion would be wrong.
- There was a reasonable expectation of privacy.
- Intrusion was substantial and highly offensive to a reasonable person.

Intent or Knowledge. The tort of intrusion to seclusion, similar to the other three that follow, requires that the defendant acted with intent to intrude or violate the plaintiff's privacy or with knowledge that actions would result in a privacy intrusion.

Reasonable Expectation of Privacy. Expanding on our earlier discussion, the level or amount of privacy we should expect depends on whether we are in what is usually considered to be a public or private place. What is done in the privacy of one's home should be entitled to more privacy than what one does in a public park or airport. However, laws may prohibit certain acts even if they occur in the privacy of one's home (see the discussion of the possession of child pornography in Chapter 10). Also, be aware that state laws can prohibit what consenting adults do in the privacy of their home. These laws usually refer to sexual activity deemed by the state to constitute "acts against nature." Similarly, the fact that an individual is in a "public" place does not deprive the person of all rights to privacy. In fact, in right to privacy cases, courts have focused on protecting the person rather than the place. In the following landmark case, the U.S. Supreme Court had to decide the privacy that an individual should expect when making a phone call in a public phone booth, even where the call involved criminal activity.

Katz v. United States
389 U.S. 347 (1967)

Facts

The petitioner, Katz, was convicted of transmitting wagering information from Los Angeles to Miami to Boston in violation of a federal statute. At trial, over the petitioner's objection, the government was permitted to introduce evidence of the phone calls obtained by FBI
agents who had attached an electronic listening and recording device to the outside of a public phone booth from which the calls had been placed. The Court of Appeals affirmed the conviction, finding there was no Fourth Amendment violation because there was no "physical entrance into the area occupied by the petitioner.” The Supreme Court granted certiorari in order to determine if the government’s eavesdropping activities violated the petitioner’s rights under Fourth Amendment “search and seizure” provisions.

**Judicial Opinion (Justice Stewart)**

Because of the misleading way the issues have been formulated, the parties have attached great significance to the telephone booth from which the petitioner placed his calls. The petitioner has strenuously argued that the booth was a “constitutionally protected area.” The Government has maintained with equal vigor that it was not. But this effort to decide whether or not a given “area,” viewed in the abstract, is “constitutionally protected” deflects attention from the problem presented by this case. For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.... But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected....

The Government stresses the fact that the telephone booth from which the petitioner made his calls was constructed partly of glass, so that he was as visible after he entered it as he would have been had he remained outside. But what he sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen. No less than an individual in a business office, in a friend’s apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call, is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.

The Government contends, however, that the activities of its agents in this case should not be tested by Fourth Amendment requirements, for the surveillance technique they employed involved no physical penetration of the telephone booth from which the petitioner placed his calls. It is true that the absence of such penetration was at one time thought to foreclose further Fourth Amendment inquiry, *Olmstead v. United States*.... For that Amendment was thought to limit only searches and seizures of tangible property. But “[t]he premise that property interests control the right of the Government to search and seize has been discredited.” *Warden v. Hayden*, 387 U. S. 294, 304, ... Thus, although a closely divided Court supposed in *Olmstead* that surveillance without any trespass and without the seizure of any material object fell outside the ambit of the Constitution, we have since departed from the narrow view on which that decision rested. Indeed, we have expressly held that the Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements, overheard without any “technical trespass under ... local property law.” *Silverman v. United States*, 365 U. S. 505, 511. Once this much is acknowledged, and once it is recognized that the Fourth Amendment protects people—and not simply “areas”—against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.
Chapter 9

The Government’s activities in electronically listening to and recording the petitioner’s words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a “search and seizure” within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not penetrate the wall of the booth can have no constitutional significance.

The question remaining for decision, then, is whether the search and seizure conducted in this case complied with constitutional standards? In that regard, the Government’s position is that its agents acted in an entirely defensible manner: They did not begin their electronic surveillance until investigation of the petitioner’s activities had established a strong probability that he was using the telephone in question to transmit gambling information to persons in other States, in violation of federal law. Moreover, the surveillance was limited, both in scope and in duration, to the specific purpose of establishing the contents of the petitioner’s unlawful telephonic communications. The agents confined their surveillance to the brief periods during which he used the telephone booth, and they took great care to overhear only conversations of the petitioner himself. Accepting this account of the Government’s actions as accurate, it is clear that this surveillance was so narrowly circumscribed that a duly authorized magistrate, properly notified of the need for such investigation, specifically informed of the basis on which it was to proceed, and clearly apprised of the precise intrusion it would entail, could constitutionally have authorized, with appropriate safeguards, the very limited search and seizure that the Government asserts in fact took place ...

The Government urges that, because its agents relied upon the decisions in Olmstead and Goldman, and because they did no more here than they might properly have done with prior judicial sanction, we should retroactively validate their conduct. That we cannot do. It is apparent that the agents in this case acted with restraint. Yet the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer. They were not required, before commencing the search, to present their estimate of probable cause for detached scrutiny by a neutral magistrate. They were not compelled, during the conduct of the search itself, to observe precise limits established in advance by a specific court order. Nor were they directed, after the search had been completed to notify the authorizing magistrate in detail of all that had been seized. In the absence of such safeguards, this Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end. Searches conducted without warrants have been held unlawful “notwithstanding facts unquestionably showing probable cause,” . . . for the Constitution requires “that the deliberate, impartial judgment of a judicial officer . . . be interposed between the citizen and the police . . . .” . . . “Over and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes,” and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.

It is difficult to imagine how any of those exceptions could ever apply to the sort of search and seizure involved in this case. Even electronic surveillance substantially contemporaneous with an individual’s arrest could hardly be deemed an “incident” of that arrest. Nor could the use of electronic surveillance without prior authorization be justified on grounds of “hot pursuit.” And, of course, the very nature of electronic surveillance precludes its use pursuant to the suspect’s consent.
The Government does not question these basic principles. Rather, it urges the creation of a new exception to cover this case. It argues that surveillance of a telephone booth should be exempted from the usual requirement of advance authorization by a magistrate upon a showing of probable cause. We cannot agree. Omission of such authorization “bypasses the safeguards provided by an objective determination of probable cause and substitutes instead the far less reliable procedure of an after-the-event justification for the . . . search, too likely to be subtly influenced by the familiar shortcomings of hindsight judgment.” *Beck v. Ohio*, 379 U.S. 89, . . .

And bypassing a neutral predetermination of the scope of a search leaves individuals secure from Fourth Amendment violations “only in the discretion of the police.” Id., at 97 . . .

These considerations do not vanish when the search in question is transferred from the setting of a home, an office, a hotel room to that of a telephone booth. Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures.

The Government agents here ignored “the procedure of antecedent justification . . . that is central to the Fourth Amendment,” a procedure that we hold to be a constitutional precondition of the kind of electronic surveillance involved in this case. Because the surveillance here failed to meet that condition, and because it led to the petitioner’s conviction, the judgment must be reversed.

IT IS SO ORDERED.

---

**Case Questions**

1. What if the government suspected illegal bets were being placed by e-mail nationwide and the FBI, without warrants, accessed and traced the e-mails resulting in criminal charges against the alleged perpetrators?
2. Would Katz’s privacy have been violated if instead of a bet he were planning a robbery?
3. Can the legal wiretapping of a “private place” ever be ethically justified?

Based on the holding in Katz, what level of privacy can we reasonably expect regarding our e-mail, use of cellular phones, and other online communications including those in chat rooms? Currently, there are no strict prohibitions imposed for collecting and using the personal information we voluntarily disclose in e-mail and other communications (later in this chapter, we discuss the laws governing unauthorized use of this information). Internet service providers (ISPs) and others utilize channels of communication easily accessible by others. Therefore, unless security measures are employed by the user to prevent access and ensure privacy, or a law recognizes a right to privacy exists, we should not expect any degree of privacy in the online information we volunteer or allow to be accessed. (*Note: Again, the best method for insuring security is encryption.*) This is similar to the easy access to cellular phone conversations.
Privacy in the Use of Cellular Phones

When using a cell phone, certainly we should expect less in the way of privacy than was afforded Katz in the phone booth, especially because scanners and other technology can be used to randomly access and intercept cell phone calls. The public or openness methods generally used to make cell calls lead to the same conclusion.

What about the courts? Some guidance regarding cell phone privacy was provided by the U.S. Supreme Court in *Bartnicki v. Vopper*, 121 S. Ct 1753 (2001) where one of the plaintiffs, the chief negotiator for a teacher’s union, made a cell phone call to another plaintiff, the union president, in which they discussed ongoing contentious union negotiations that had also been widely reported in the media. An unknown person illegally intercepted the call and mailed a tape of it to one of the defendants. He in turn sent it to the other defendant, a talk show host who played it on his radio program. The plaintiffs sued claiming their privacy rights had been violated under state and federal wiretap laws (Electronic Communications Privacy Act, discussed later). The defendants argued that because the conversation contained information of importance to the public, they were entitled to First Amendment protection. The Court agreed with the defendants and decided, at least based on the facts of this case, that the privacy concerns of the plaintiffs were outweighed by the freedom of speech and press rights of the defendants to communicate or publish information, even though wrongfully intercepted, that was truthful and of significant interest to the public.

As far as the privacy rights of employees are concerned, we will discover that there is virtually little or no reasonable expectation of privacy in the workplace, and if an employee were to be successful in proving an invasion of a right to workplace privacy, probably *Intrusion upon Seclusion* provides the best (remedy) theory for recovery.

**Substantial and Highly Offensive to a Reasonable Person.** Most of the case law and the Restatement (Second) of Torts concerning this tort require that the defendant’s conduct and resultant intrusion shock or outrage the conscience of a reasonable person. The actions of the FBI in the Katz case would satisfy this element. Similarly, as we see later with workplace privacy, monitoring telephone or e-mail messages without justification or consent would probably also constitute an intrusion sufficient for this element.

**Public Disclosure of Private Facts Causing Injury to Reputation**

This tort allows recovery when highly personal facts or information about another are publicly disclosed or transmitted whereby injury to reputation results. In some instances, this tort is associated with the tort of defamation, and both may be used as separate causes of action arising out of the same case.

In addition to the elements of “intent or knowledge” and “highly offensive to a reasonable person” previously discussed, the public disclosure of private facts causing injury to reputation requires the following:
• The facts must be private.
• Communication or publicity must be disclosed to a significant segment of the community.

**Facts Must Be Private.** If the information disclosed were obtained with consent, voluntarily, or was already in the public domain, this tort likely will not be successful. This can result when we sign a consent form authorizing the release of personal information about us related to medical or insurance reports. It could also be true regarding highly personal information we volunteer to ISPs or companies operating online. This information ends up stored in their vast databases, available for any number of purposes, including the sale to others.

If the information is not obtained as described and subsequently is disclosed, the issue again focuses on establishing that the plaintiff had a reasonable expectation the facts disclosed would be kept private.

**Communication or Publicity to a Significant Segment of the Community.** Recovery here is based on disclosure to a large enough group of people so the information about the plaintiff becomes common knowledge. Therefore, it would be insufficient “to communicate a fact concerning the plaintiff’s private life to a single person or even a small group of persons” [Restatement (Second) of Torts].

**Publicity Placing Another in a False Light**

This tort also is associated with the tort of defamation and involves falsely connecting a person to an immoral, illegal, or embarrassing situation resulting in injury to one’s reputation. In general, the elements of this tort mirror those already discussed. To date, it has not been the subject of much, if any, litigation involving the invasion of privacy in cyberspace.

**Misappropriation of a Person’s Name or Likeness Causing Injury to Reputation**

This tort usually applies in cases where the name or picture of a living person is used for commercial (non-newsworthy) purposes without the person’s permission or consent. In some states, such as New York, it can result in both criminal and civil liability. Consider *Stern v. Delphi Services Corporation*, 626 N.Y.S. 2d 694 (N.Y. Sup. Ct. 1995), where, as a publicity stunt, Howard Stern, the plaintiff and controversial radio “shock jock” and self-proclaimed “king of all media,” facetiously ran for governor of New York. The defendant operated an online news service and to promote its products, he took out a full-page ad in two New York publications in which a photo of Stern in leather pants with his buttocks exposed ran without his permission. Stern alleged that the picture violated a New York statute prohibiting commercial use of an individual’s name or picture without permission. The statute provided for an “incidental use exception” that allowed news providers to publicize newsworthy communications. Such was the case here. Stern’s candidacy was newsworthy because of his celebrity and candidacy. Therefore, his right to privacy was not violated. The court stated that to restrict the defendant from informing the public of the nature and sub-
object of its service would constitute an impermissible restriction of its First Amendment rights. Cases like Stern demonstrate the difficulty and exceptions courts can recognize when dealing with the privacy rights of celebrities.

Another interesting case involving this tort and the duty of a pharmacy to maintain the confidentiality of information concerning its customers is Weld v. CVS Pharmacy, Inc., et al., 1999 WL 494114 (Mass. Sup. Ct. June 29, 1999), where CVS, without the knowledge or consent of its customers, released their names, addresses, phone numbers, and other personal information, including the nature of their illnesses and diseases, to drug manufacturers, who then sent to them information specific to their ailment. The court allowed the case to proceed to trial to determine if the tort of misappropriation of private information and an invasion of privacy occurred given the fact that a pharmacy owes a duty of confidentiality to its customers.

A similar case at the federal level, In the Matter of Eli Lilly, Docket No. 0123214, January 18, 2002, involved a complaint brought by the FTC against Eli Lilly, Inc., a huge drug company that manufactures drugs including the antidepressant Prozac. Lilly maintained and offered several Web sites, including http://www.prozac.com, which provided information about the drug Prozac and also offered an e-mail prescription refill reminder service called Medi-messenger. Some 669 Prozac users opted for the service and automatically received personal e-mail reminders to take their medication or to refill their prescriptions. However, in June 2001, a decision was made to terminate the program, and one of Lilly’s employees created a program to e-mail each customer of the site’s termination. Instead, the employee accidentally sent the e-mail to all 669 members simultaneously, rather than individually, thereby disclosing their identities to one another. Despite Lilly’s claims that they had implemented adequate customer privacy and confidentiality policies, the FTC disagreed, deciding Lilly’s actions were deceptive because it failed to maintain or implement adequate internal procedures including proper employee training to protect and ensure the privacy and confidentiality of the personal information. Lilly admitted they were negligent and agreed to create and implement a new information security program.

This case is significant because it represents a shift by the FTC in its efforts to protect consumer privacy. It appears that liability for privacy violations of the type involved in CVS and Lilly will arise even where the defendant’s actions, although unintentional, demonstrated a lack of reasonable care and resulted in actionable negligence and potential liability. Recall that all four common law torts for invasion of privacy require the element of intent.

**Federal Privacy Laws**

Congress began passing laws designed to protect privacy in the 1970s (see Figure 9.1). These laws deal primarily with the requirements for keeping and using personal data about individuals by the government. In this part of the chapter we focus on the most significant of those acts as well as those that affect nongovernment or private
entities. Keep in mind that the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act) of 2001 has amended many of these.


The Privacy Protection Act (PPA) applies to law enforcement agencies and allows Fourth Amendment protection against the unreasonable searches and seizures of:

> Work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public, a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate commerce.

The PPA could apply to those qualifying as electronic publishers who use the Internet for the interstate transmission of their messages. If there were probable cause to believe the materials sought from these publishers were being used for a criminal purpose, a court would likely uphold a search of them as long as Fourth Amendment requirements were met. The same would be true if the search was necessary to prevent a person’s injury or death. (See the Scarfo case in Chapter 12, “Internet and Information Security.”)

**Privacy Act of 1974, 5 U.S.C. § 552a Amended**

The Privacy Act was passed because Congress was concerned with curbing the surveillance and investigation of individuals by federal agencies precipitated by the Watergate break-in scandal during the Nixon administration, and also with the potential negative impact on privacy rights that could arise from the government’s increased use of computers to access, collect, and store personal data and its ability to retrieve it by simply using an individual’s Social Security number.
Nearly thirty years later, the USA Patriot Act has diminished those concerns wherever outweighed by interests of national security. The Privacy Act has been described as a kind of “omnibus” code of fair information practices (discussed later) designed to regulate the collection, maintenance, use, and disclosure of personal information by federal agencies by establishing requirements that must be satisfied before government agencies or departments can disclose records and documents in their possession that contain personal information about individuals. The act only applies to records and documents that identify an individual by name, Social Security number, or other means of personal identification such as a photograph, fingerprint, or voiceprint. Thus, in order for the act to apply to the Internet, personal information about a person would have to be stored in a file containing one of these identifying features. The individual’s name alone would be insufficient for the act to apply.

In addition, the act requires the agency or department to do the following:

1. Obtain the written consent of the individual unless the purpose of the disclosure is consistent with that for which the records are being retained.
2. Furnish copies of the records to the individual upon request.
3. Allow the individual to correct any misinformation contained in the records.
4. Make a reasonable effort to inform the individual that his or her records have been disclosed.

In general, the exceptions to these requirements apply to certain government law enforcement activities, situations that concern the health or safety of an individual, and court-ordered disclosures. Violations of the act can result in lawsuits by the injured party against the agency for money damages, remedies at equity such as an injunction, or both.

**Cable Communications Protection Act (CCPA) (1984), 47 U.S.C. § 551**

The Cable Communications Protection Act (CCPA) applies to cable television operators and is concerned with the privacy rights a subscriber should expect regarding personal data or information about them that a cable television operator gathers. In general, the operator is required to do the following:

1. Obtain the permission of its subscribers before collecting personal data about them.
2. Notify subscribers annually regarding the extent to which personal information about them is used or disclosed, and the purposes for which it is gathered.
3. Allow the subscriber to examine the data and make corrections of any errors or mistakes.
4. Not disclose the data except as may be required by law or court order.

(Note: This requirement also applies to government requests for personal information about cable subscribers.)

Failure to follow these requirements can result in lawsuits by affected subscribers. Seemingly, the CCPA could apply to the operator of a Web site that offers cablelike
entertainment (adult or otherwise) or goods and services, and where its visitors wish to remain anonymous.


The Video Privacy Protection Act (VPPA) expands the Cable Communications Protection Act. Specifically, it prohibits the use and disclosure of personal information about the videocassettes and related products an individual rents or purchases unless their written permission is obtained. This act could be applied to rentals and purchases of videos and related products via the Internet.


The Telephone Consumer Protection Act (TCPA) was passed as a direct result of the telemarketing activities arising from the transmission of telephone solicitations originating from automatic dialers. TheTCPA directs the Federal Communications Commission (FCC) to promulgate and implement rules and regulations directed at these solicitations. Basically, the TCPA provides the following:

1. It is illegal to make a phone call by means of an automatic dialing system or prerecorded (or artificial) voice that results in the party called being charged for the call. (This also applies to calls made to a cellular phone number.)
2. It prohibits the use of any device to send an unsolicited advertisement to a telephone facsimile machine.
3. Companies engaging in telephone telemarketing are required to set up “do not call” lists for consumers who do not wish to receive these types of calls.

Consumers also have the right to have their names removed or excluded from existing lists. These “do not call” lists generally allow a telemarketer one call before civil liability arises. In general, industry efforts have been virtually ineffective, which has resulted in more than half of the states establishing their own “do not call lists.” In December 2002, the FTC amended the Telemarketing Sales Rule to require and establish a national “do not call” registry effective July 2003. Many would like a similar “do not spam” rule to apply to spamming (the mass or bulk mailing of unsolicited e-mails containing advertisements for goods or services). Spamming is discussed in greater detail later in this chapter.

It should be noted that a federal district court has given exclusive jurisdiction to the states in suits brought under the TCPA. [*Eriencet, Inc., et al. v. Velocity Net, Inc., et al., 1998 U.S. App. Lexis 23931 (3rd Cir., September 25, 1998)*].

**Federal Legislation: Credit and Financial Records**


The purpose of the Fair Credit Reporting Act (FCRA) is to ensure that the credit reports furnished by consumer credit reporting agencies, including requests sent
online, are accurate, impartial, and respect privacy. Also, in general, before an agency can release or use credit information about an individual, his or her permission must be obtained. An example would be when a credit card, insurance company, or financial institution uses credit information to profile or "prescreen" consumers for unsolicited e-mail (spam) marketing offers.

The FCRA also gives consumers the right to obtain information about their credit status from credit bureaus and check or correct any errors that exist. Another provision requires credit-reporting agencies to maintain a toll-free phone number so representatives are available to consumers seeking to discuss their credit reports. The Federal Trade Commission (FTC) has jurisdiction over the FCRA, usually basing its complaints under Section 5 of its regulations that prohibit unfair or deceptive business practices that affect business.

Failure to comply with the FCRA requirements can result in civil and criminal liability. In 2000, three major credit-reporting agencies, Equifax, Trans Union, and Experian, entered into a consent decree with the Federal Trade Commission whereby they agreed to pay $2.5 million to settle claims that they violated the FCRA for not maintaining a consumer toll-free phone number allegedly by blocking millions of consumer calls from reaching the number and by keeping others on hold for extraordinarily long periods of time.


The primary purpose of the Computer Fraud and Abuse Act (also discussed in Chapter 13, "Internet and Computer Crime") is to protect national security by prohibiting the intentional access of data stored in computers belonging to or benefiting the U.S. government. The CFFA makes it a felony for an individual to obtain this data without authority. Of significance to our discussion of privacy is another provision of the act that makes it a felony to intentionally access personal identifiable information about a consumer contained in the financial records of a financial institution or in a file of a consumer reporting agency.

**FEDERAL LEGISLATION: PRIVACY IN PERSONAL FINANCIAL INFORMATION**

Congress has passed other federal laws intended to protect privacy rights in personal identifiable information (PII) contained in our financial records and data. These include the Bank Secrecy Act of 1970 that essentially makes it illegal to launder money and use secret foreign bank accounts for illegal purposes. It also requires that financial institutions (banks, credit unions, etc.) and nonfinancial institutions (casinos, brokerages, etc.) report to the U.S. Treasury Department any cash transaction over $10,000. The Treasury Department can share this information with other law enforcement agencies.

It should be obvious that this act would be extremely beneficial in helping law enforcement and other agencies (charged with protecting homeland security) in their efforts to follow any trail of money destined for enemies of the United States or...
monies illegally obtained through fraudulent schemes (insider trading, tax fraud, etc.). The act also authorizes the Treasury Department to require financial institutions to keep records of their customers’ personal financial transactions, including those conducted online that have “a high degree of usefulness in criminal, tax and regulatory investigations and proceedings.”

Additionally, the Treasury is authorized to require that a financial institution report to the Treasury any “suspicious transaction” carried out by a customer that could result in or be relevant to possible violations of laws or regulations. The privacy concern here is that this is done without the knowledge or permission of the customer and the law enforcement agency does not have to be suspicious of an actual crime before it accesses a report and no court order, search warrant, subpoena, or written request is needed.

Brief mention should also be made here of the Right to Financial Privacy Act of 1978, 29 U.S.C. § 3401, passed by Congress to provide some semblance of privacy protection to customers of banks and other financial institutions by requiring the government, subject to exceptions under the Patriot Act, to obtain a search warrant before being allowed to access financial records and information.

The most significant federal law passed by Congress pertaining to privacy protection for the disclosure and use of PII collected and contained in financial records is the Gramm-Leach-Bliley Act (GLB) of 1999, also known as the Financial Services Modernization Act of 1999.


As you study the GLB Act, keep in mind that the Computer Fraud and Abuse Act makes it a felony to intentionally access, without authorization, personal identifiable information about a consumer contained in the financial records of a financial institution or credit bureau. Also, be aware that the major federal administrative agencies that have regulatory and enforcement powers regarding the GLB include the Securities and Exchange Commission, the Federal Reserve Board, and the Federal Trade Commission.

The GLB Act applies to all financial institutions that offer financial goods and services including but not limited to banks, credit unions, mortgage companies, insurance companies, and brokerages. Specifically, Title V of the GLB Act provides privacy protection for personal identifiable information (PII) collected by financial institutions. The GLB Act effectively repealed the sixty-six-year-old Glass-Steagall Act that prohibited financial institutions from affiliating or combining with one another and disclosing and sharing PII about their customers. The GLB Act now allows both affiliations and the sharing of information. Examples of acceptable affiliations include Charles Schwab and the U.S. Trust Company, Citizens Bank and Travelers Insurance, and Solomon-Barney and Citicorp.
Title V of the GLB Act provides notice and consent requirements that financial institutions must satisfy before they can disclose or share personal identifiable financial information about their customers with nonaffiliated businesses. If the GLB Act notice and consent requirements are met (discussed later), these institutions may share personal financial information about their customers with each other. Such information would include the name of the customer along with his or her account balance. The same is true for ISPs and nonaffiliated companies with whom the financial institution has an agreement, the terms of which allow these companies to market their goods and services to customers of the financial institution.

**Notice and Consent Requirements: Nonaffiliates**

At the beginning (and annually thereafter) of the business relationship between the customer and its bank or other financial institution, the GLB Act requires the bank to provide the customer with a privacy notice that indicates how it collects, discloses, and uses their “nonpublic” or personal identifiable (financial) information (PII). The institution must also provide the customer with the opportunity and methods to be used in order to “opt-out” or deny permission to the bank to share PII with nonaffiliates. Typically these methods include:

- Letter or form provided by the institution
- Toll-free phone number to be called
- Online, if this is the usual method for doing business with the institution.

Note that if a specific method for opting out is prescribed and not followed by the customer, the institution may or may not accept it.

In any event, the procedure clearly puts the burden on the customer to take appropriate action, and recent estimates indicate that only about 5 percent have met that burden and have actually opted out. Some of the reasons privacy advocates have advanced for this low rate include consumer indifference, lack of knowledge of the privacy issues surrounding their financial information, and the inconvenience an opt-out policy presents. As a result, these advocates have criticized the GLB Act as being ineffective in protecting privacy rights and, along with members of Congress, have sought, albeit unsuccessfully, new federal legislation that would require financial institutions to implement an “opt-in” policy. This would require a financial institution to obtain permission from the customer before being allowed to collect and use the information, effectively shifting the burden.

Some states such as Vermont and New Mexico have adopted “opt-in” policies. It is important to note, if state law provides greater privacy protection for consumers, the GLB Act provides that such laws preempt its application. You should be aware that the GLB Act also contains requirements that attempt to prevent the crimes of identity theft and “pretexting,” both of which severely threaten and invade our privacy.

**Identity Theft**

A major threat to privacy is identity theft as it relates to personal financial information. Prohibited under Title V of the GLB, identity theft occurs when personal identifiable
information (PII) such as an account number or Social Security number is stolen and used to obtain financial services. Examples include obtaining a loan, credit card, or bank account in the name of the person whose identity was stolen. The Identity Theft and Assumption Deterrence Act of 1999, 18 U.S.C. § 1028, gives the FTC jurisdiction to process identity theft complaints and to assist victims and direct them to the proper law enforcement agency.

In 2001, the FTC reported it had received complaints from over 86,000 victims of identity theft. In Chapter 13, “Internet and Computer Crime,” you will learn more about this crime.

**Pretexting**

Pretexting is also prohibited under Title V of the GLB Act and results when personal financial information such as a bank account number is fraudulently or falsely obtained by contacting the victim’s bank or financial institution under the pretext of being or impersonating the actual customer.

**FEDERAL LEGISLATION: PRIVACY IN HEALTH AND MEDICAL RECORDS**

Personal identifiable information (PII) contained in our health and medical records has also become a major focus of privacy concerns. In response, Congress passed the very complicated Health Insurance Portability and Accountability Act (HIPAA) of 1996, P.L. 104-191.

**Health Insurance Portability and Accountability Act (HIPAA) of 1996, P.L. 104-191**

HIPAA applies to what it classifies as “covered entities” including health care providers, health care clearinghouses, and health plans, including those offered by employers to their employees, as well as to others providing services to them who transmit health information electronically. Essentially, HIPAA covers the receipt, transmittal, and disclosure of personal health information and data related to health plans, health care clearinghouses, and health care providers (hospitals, physicians, insurance companies, employers, etc.) that use electronic communications for processing and disclosing personal health information (PHI) surrounding health claims, payments, and other related services. HIPAA attempts to protect the confidentiality of our health records without creating obstacles for quality health care. Its provisions were so extensive and difficult, extra time was needed for implementation and compliance. HIPAA did not become fully effective until April 14, 2003. HIPAA will be implemented by the U.S. Department of Health and Human Services (HHS).

In general, HIPAA requires a covered entity to give written notice to a patient at the time of their treatment as to how their personal health information (PHI) will be used and disclosed. It also gives a patient the right to receive a copy of their medical records and inspect and correct PHI if they so choose. Further, HIPAA requires that covered entities give patients an opportunity to opt in (not opt out as allowed under
GLB) by giving their written authorization or permission before releasing patient related PHI. Originally, HIPAA distinguished between routine matters related to treatment, payment, and health care operations for which patient consent was to be required. However, in August 2002, HHS promulgated an amendment eliminating the strict requirement that a health care provider obtain a patient’s written consent for information related to routine matters regarding treatment, payment, and health care operations. Now, a health care provider need only make a “good faith” effort to obtain consent before disclosing or using this information. Legal challenges to this amendment are likely because it appears to diminish Congress’ intent in passing HIPAA to protect patient privacy. A final point to remember is that state laws that provide greater protection than HIPAA and GLB preempt and prevail over them.

**Privacy Protection for Children from the Collection of Online Personal Information**


The Children’s Online Privacy Protection Act (COPPA) protects children under age thirteen and applies to commercial operators that collect or store data containing personal identifiable information (PII) concerning children who visit or use their Web sites. The FTC is charged with implementing COPPA and has established requirements that these operators must satisfy before they collect PII from children under age thirteen. Essentially, they must:

- Provide a clear and conspicuous link, on their home page and/or wherever such information is collected, to a description of their information collection practices.
- Indicate what types of information is collected and how it is to be used.
- Indicate if it will be disclosed to third parties along with a description of the nature of the third party’s business.

COPPA’s most important privacy protection provision requires that operators obtain verifiable parental consent before collecting, disclosing, or using PII obtained from children. Although COPPA allows a parent to indicate consent via an e-mail, the operator must confirm the consent by phone, letter, or e-mail sent to the parent.

Since its passage, the FTC has successfully brought several complaints under COPPA. The first, and one of the most publicized, was FTC v. Toysmart.com, LLC, District of Massachusetts, Civil Action No. 00-11341-RGS, 2000. Toysmart.com was a company that sold educational toys online. Its privacy statement contained a promise that it would never disclose or sell PII it collected from its customers, some of whom were children under age thirteen. Toysmart.com filed for bankruptcy and, pending that proceeding, wanted to sell its customer databases containing the customer PII. The FTC claimed this was a misrepresentation and sought to prevent the sale, seeking an injunction alleging unfair and deceptive business practices under Section 5 of the FTC Act and a failure to obtain verifiable parental consent as required by COPPA. The FTC succeeded in enjoining the sale except to a “qualified buyer” who would have to agree to abide by the promise contained in the privacy statement. Subsequently, the
settlement was challenged by thirty-nine state attorneys general who alleged that any sale even to a qualified buyer would violate COPPA as well as Toysmart’s policy and promise. The U.S. Bankruptcy Court agreed and, in August 2000, overturned the settlement requiring Toysmart to obtain court approval before selling its databases.

COPPA: Safe Harbor

COPPA provides a safe harbor for those operators who engage in some form of self-regulation program such as those offered by so-called seal organizations sanctioned by the FTC program. Examples include the Children’s Advertising Review Unit of the Council of Better Business Bureaus, TRUSTe, and the Entertainment Software Rating Board that establish policies and rules for meeting the privacy provisions of statutes like COPPA. The FTC has also set up an informational link on its home page for children, parents, operators, and service providers called Kidz Privacy.

The Electronic Communications Privacy Act (ECPA) of 1986, 18 U.S.C § 2510

One of the most important federal statutes regarding privacy in cyberspace is the Electronic Communications Privacy Act (ECPA) of 1986. In 1968, no doubt influenced by cases including *Katz v. United States* (discussed earlier in this chapter) that demonstrated the ability of the government to monitor and record telephone conversations, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act (18 U.S.C. § 2510), the so-called wiretap statute. This statute established Fourth Amendment requirements that government agencies would have to satisfy in order to carry out legal wiretaps. These included obtaining a valid search warrant
based on a showing of probable cause that the phone call to be intercepted was related to a criminal activity.

By the 1980s, advancements in technology and the creation of new and more sophisticated modes of wire and electronic communications, including e-mail, caused concerns that existing wiretap laws were inadequate to protect the rights of individuals. Congress responded by passing the ECPA, which amended the Omnibus Crime Control and Safe Streets Act. The ECPA applies to ISPs and other commercial online service providers engaged in the transmission, interception, and storage of electronic communications, including e-mail “to the public” that affects interstate or foreign commerce.

The meaning of “to the public” under the ECPA was a major issue before the court in Andersen Consulting LLP v. UOP, 991 Fed. Supp. 1041 (N.D. Ill. 1998). In Andersen, the defendant maintained an internal e-mail system and allowed the plaintiff to use it. The defendant disclosed some of the plaintiff’s e-mail messages to a newspaper that published them and the plaintiff sued under the ECPA. The court dismissed the suit, interpreting the phrase “to the public” as meaning the “community at large.” Here, the defendant intended its e-mail system to be for internal communication purposes and not for transmission to the public or community at large. The defendant certainly had not intended to affect interstate commerce. Therefore, the disclosure did not violate the ECPA.

Essentially, the ECPA contains three major provisions, Title I (also known as the Wiretap Act) applies to the interception and disclosure of wire, oral, and electronic communications. Title II (also known the Stored Communications Act) applies to stored wire, transactional, and electronic communications. Title III (also referred to as the Pen Register Act) applies to wiretaps via telephone pen registers and trap and trace devices. Violations of the ECPA can result in criminal and civil liability. Note that the ECPA does not, in the absence of an agreement to the contrary, prohibit disclosure of the contents of an e-mail message by the intended recipient to another person.

**Title I (§§ 2510–2522) — Interception and Disclosure of Wire, Oral, and Electronic Communications.** Title I prohibits the unauthorized interception and disclosure of wire, oral, and electronic communications. The ECPA defines an electronic communication as:

Any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photooptical system that affects interstate or foreign commerce.

Examples include transmissions by radio paging devices (excluding “tone-only” devices), cellular phones, computer-generated transmissions, and e-mail. The ECPA covers all communication carriers or persons who provide or operate facilities for communications that affect interstate or foreign commerce.

Specifically, Title I prohibits, with exceptions:

1. Any person from intentionally intercepting any wire, oral, or electronic communication;
2. Any person from intentionally using or disclosing the contents of any wire, oral, or electronic communication to another person;

3. An Internet service provider (ISP) from intentionally disclosing the contents of a communication to any person or entity other than the addressee or intended recipient.

In *McVeigh v. Cohen et al.*, 983 F. Supp. 215 (D.D.C., 1998), the plaintiff, Timothy McVeigh, was discharged from the U.S. Navy because he was gay, a fact disclosed to the navy by America Online (AOL), an ISP. AOL had discovered McVeigh’s sexual orientation after identifying him as the sender of an anonymous e-mail and as an individual described in its membership directory as gay. In issuing a preliminary injunction preventing the navy from discharging McVeigh, the Court of Appeals ruled the navy was in violation of its “Don’t ask, don’t tell” policy. The Court was also aided in its decision by the actions of AOL in intentionally disclosing information about McVeigh and his e-mail, resulting in a direct violation of the ECPA.

*Note:* The ECPA does not prohibit access or disclosure of electronic communications placed on a site intended to be readily accessible by the public.

There are four *major* exceptions to Title I:

1. Internet service providers (ISPs)
2. Business Extension Rule, or “Ordinary Course of Business”
3. Prior consent to interception of electronic communications
4. Government and law enforcement agencies—interception and disclosure of electronic communications. (These exceptions also apply to Title II and III.)

1. **Internet Service Providers (ISPs).** An online operator, officer, employee, or agent of a provider of wire or electronic communication service may, in the normal course of employment, intercept, disclose, or use an electronic communication “which is a necessary incident to the rendition of” their service or to the “protection of the rights or property of the provider of that service.” (*Note:* Random observing or monitoring of a communication are not allowed under this exception except for mechanical or quality control purposes.) This exception would apply to outside e-mail service providers such as Prodigy, CompuServe, and America Online, as well as to an internal e-mail system operated by the employer. In *United States v. Mullins*, 992 F. 2d 1472 (9th Cir. 1992), an employee and agent of American Airlines was investigating discrepancies in reservations being made by a travel agent on an online travel reservations system maintained by American. The employee intercepted some of these reservations and the travel agent sued, arguing the employee’s actions violated Title I of the ECPA. The court disagreed, deciding that American Airlines was a service provider acting to protect its rights and property interests. Therefore, the interception of the communication was allowable under the exception just described and did not violate the ECPA.

2. **Business Extension Rule or Ordinary Course of Business.** The business extension rule focuses on the ECPA section that requires a plaintiff to prove the defendant used an “electronic, mechanical, or other device,” capable of intercepting an electronic communication. Specifically, it exempts from liability under the ECPA any device fur-
nished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of business and being used by the subscriber or user in the ordinary course of its business.

This exception would allow the interception of e-mail and other communications by an employer, provided certain qualifications are met. More follows in the discussion of workplace privacy later in this chapter. For now, suffice it to say that the employer would have to prove it had established a monitoring policy and certain employees knew about it in advance of the interception, and that the interception was business related. Therefore, it appears an employer could monitor an employee’s phone calls or e-mail messages in order to make sure they were business related and not purely “personal” in nature.

3. Prior Consent. The interception of an electronic communication is permitted when one of the parties to the communication, either the sender or the recipient, has given prior consent to the interception unless the communication is intercepted for purposes of committing a crime or tort.

4. Government and Law Enforcement Agencies—Interception and Disclosure of Electronic Communications. Here the ECPA distinguishes between an electronic communication accidentally intercepted by a service provider and those sought from an ISP or other provider by a government or law enforcement agency official.

A service provider who accidentally intercepts a communication containing evidence of an illegal act may, without liability under the ECPA, disclose the communication to the proper authorities. However, law enforcement officials must follow the provisions of the ECPA. Essentially, they require the official to apply to a judge for a court order, search warrant, or, in the case of private documents, a subpoena. In the application, the official will have to establish there is sufficient probable cause to believe the person named in the application is, has, or is about to commit a crime. The official will also have to describe in particular detail the place and items to be searched.

If the communication sought is associated with an emergency situation that poses an immediate threat of death or serious injury to a person, a threat to national security, or involves criminal activity associated with organized crime, the interception may occur without the application and court order, warrant, or subpoena. However, within forty-eight hours after the interception, the agent must then comply with the above application procedure. If the application is not approved and a court order, warrant, or subpoena is not issued, the interception will be declared to have been obtained in violation of the ECPA and would be, most likely, inadmissible in a criminal prosecution brought against the person who was the subject of the application.

In most cases where the government has requested access to a subscriber’s e-mail messages or other stored data, the ECPA requires the service provider to notify the subscriber of the request. The subscriber then has fourteen days from the date of the notice to challenge the request in a court proceeding. An interesting question is posed by an electronic communication containing a message that is encrypted. Obviously, a service provider could not accidentally intercept this type of message.
What about a law enforcement agency seeking to intercept a message it believes contains evidence of a criminal activity? Currently, there is no law that expressly gives law enforcement officials the right to access encrypted messages even with a court order. The FBI and other law enforcement agencies have asked for laws requiring that encryption software be sold with key features (a kind of “back door”) that would allow a message to be decrypted and accessible by law enforcement agencies. In *U.S. v. Scarfo*, presented in Chapter 12, “Internet and Information Security,” you will discover that the court exercised its interpretive muscle to fashion a unique application of a federal statute, the Classified Information Procedures Act, in order to strike a balance between individual privacy rights and the need for law enforcement agencies to employ new technology to investigate and prosecute criminal activity, especially post 9/11. The decision in *Scarfo* appears to have provided at least a partial answer to the FBI’s request. In Chapter 12, you will also learn about Carnivore (also known by its less ominous name, DCS 1000) and other surveillance key logger tools the FBI and law enforcement agencies use to help fight terrorism and other crimes. Here, we briefly mention the privacy concerns raised by Carnivore.

**Carnivore**

*Carnivore* is a device the FBI likens to a pen register (a device that records phone numbers dialed from another phone) that allows the FBI pursuant to a court order to search (“sniff”) and sift through the e-mail and other Internet traffic passing through a suspect’s ISP and intercept what it believes indicates evidence of criminal activities. One of the major privacy concerns raised is that *all* traffic is searched, even that of individuals not named in the original court order. The FBI is able to obtain sender and recipient’s addresses as well as the subject matter contained in their e-mail.

This being the case, privacy advocates and critics of Carnivore are concerned that the volume and extent of the data gathered pose privacy threats to innocent citizens and liken Carnivore to a wiretap for which stricter Fourth Amendment scrutiny would be required. The FBI claims that its use of electronic surveillance has led to over 25,000 criminal convictions in the past thirteen years and is therefore vital to its crime fighting efforts.

Of course, remember in the interest of national security the USA Patriot Act has increased the authority and ability of the federal government to monitor and access electronic communications and Internet activities. Some have observed this to result in a diminution of Fourth Amendment and privacy rights and protections.

**Title II (§ 2701)—Unlawful Access to Stored Communications.** The purpose of Title II is to protect data stored in transit and at the point of destination from being accessed and disclosed. This usually involves data stored in RAM (random access memory) or on computer discs and other similar devices.

Subject to exceptions similar to those under Title I, § 2701 basically does the following:

1. It prohibits any person from intentionally accessing without authorization a facility through which an electronic communication service is provided or
intentionally exceeding authorization to access that facility and thereby obtaining, altering, or preventing authorized access to a wire or electronic communication while it is in electronic storage in such a system.

Although similar to those provided under Title I, one additional exception should be mentioned: § 2701 (c) (2) exempts from liability conduct authorized by a user of a wire or electronic communication service with respect to a communication of or intended for that user. The application of this exception and the ECPA are discussed later in this chapter in the DoubleClick case and in the Konop case dealing with workplace privacy.

It was also an issue in Sega Enterprises v. MAPHIA, 948 F. Supp. 923 (N.D. Ca. 1996). In deciding the copyright infringement issue before it, the court had to look at whether Sega’s employee’s actions in using a pseudonym to access data stored on MAPHIA’s bulletin board system (BBS) violated this section of the ECPA. The BBS was readily accessible to the public at large by use of pseudonyms and Sega had collected the information by having one of its employees gain access to the BBS under a pseudonym using information supplied by an authorized user who was an informant. Because the data were available on a public BBS, the court decided Sega’s actions did not violate this section of the ECPA.

2. It prohibits a person or entity providing an electronic communication service to the public from knowingly divulging to any person or entity the contents of any communication while in electronic storage by that service.

3. A person or entity providing remote computing service to the public is prohibited from knowingly divulging to any person or entity the contents of any communication that is carried or maintained on that service. In the following class action case, the court had to decide if a company’s use and placement of cookies on the plaintiff’s computer hard drives in order to collect nonpersonal identifiable information violated Title II of the ECPA or met one of its exceptions.

In Re DoubleClick Inc., Privacy Litigation
154 F. Supp. 2d 497 (S.D. N.Y., 2001)

Facts

DoubleClick is the largest provider of Internet advertising products and services in the world, specializing in collecting, compiling, and analyzing nonpersonal identifiable information about Internet users and using it to target online advertising. It promises its clients to place ads in front of viewers who match their clients’ demographic target and has placed billions of ads online. Its services reach a majority of the Internet users in the United States.

By placing cookies on the hard drives of its users’ computers, DoubleClick is able to collect the information when the user accesses a DoubleClick affiliate. A user may take simple
steps to prevent DoubleClick’s use of cookies by “opting out” (denying permission to
place them on the hard drive) or by reconfiguring the browsers on their computers in
order to block any cookies from being deposited.

The plaintiffs brought this action on behalf of themselves and all others who, since Janu­
ary 1, 1996, have had information collected about them by Doubleclick as a result of viewing
products or services on the Internet or who have had cookies placed on their computer hard
drives by DoubleClick. The plaintiffs allege that these actions constituted an invasion of their
privacy and violated Title II of the ECPA, § 2701 that prohibits unauthorized access of
stored communications. They also alleged violations of other federal and state laws. Dou­
bleClick argued that because its clients consented to the gathering of the information, it met
the requirements of the prior consent exception. In seeking a motion to dismiss, . . .

Judicial Opinion (District Judge Naomi Reice Buchwald)

Assuming the communications are considered to be in “electronic storage,” it appears that
DoubleClick’s conduct constitutes an offense under the Electronic Communications Pri­

§ 2701 (a) provides:

 Whoever intentionally accesses without authorization a facility through which an
electronic information service is provided and thereby obtains access to a wire or
electronic communication while it is in electronic storage in such system, shall be
punished.

Subsection (a) shall not apply with respect to conduct authorized by a user of
that [wire or electronic communication] service with respect to a communication
of or intended for that user.

Therefore, the issue is whether DoubleClick’s conduct falls within the exception. The
issue has three parts: (1) what is the relevant electronic communication service? (2) were
DoubleClick-affiliated websites “users” of this service? (3) did the DoubleClick-affiliated
websites give DoubleClick sufficient authorization to access plaintiffs’ stored electronic
communications “intended” for those websites? Obviously, in the broad sense, the
“Internet” is the relevant communications service. However, it is important that we define
Internet service. Plaintiff argues that the electronic communication service is “Internet
access” and the “ISP” (Internet Service Provider). The difference is important. An ISP is
an entity that provides access to the Internet (America Online, etc.). Access to the Internet
is the service an ISP provides. Therefore, the “service that provides to users thereof the
ability to send or receive wire or electronic communications” is “Internet Access.”

The ECPA defines a “user” as “any person who uses an electronic communication
service; and is duly authorized by the provider of such service to engage in such use.”
DoubleClick-affiliated websites appear to be users. They are “entities” that use Internet
access and are authorized to use Internet access by ISPs to which they subscribe. One could
imagine a facially sensible argument that websites are not “users” of Internet access because
they are passive storage receptacles for information; the human is the “user” and the web­
site is what is used. However, the Internet’s engineering belies this description. Indeed, no
direct connection ever exists between the human user and the website. Rather, the human
Chapter 9 Privacy

sends a request to which the website must actively respond. Indeed, websites are among the most active “users” of Internet access—their existence and utility depend on it. Therefore, we find as a matter of law that the DoubleClick affiliated websites are “users” of Internet access under the ECPA.

Plaintiffs have proffered no proofs to support their bare assertion that DoubleClick’s access was unauthorized. Every fact they do allege supports the inference that the DoubleClick-affiliated Web sites did authorize DoubleClick’s access.

The very reason clients hire DoubleClick is to target advertisements based on users’ demographic profiles. Title II in no way outlaws collecting personally identifiable information or placing cookies. Therefore, we find that the DoubleClick-affiliated Web sites consented to Doubleclick’s access of plaintiffs’ communications to them. DoubleClick did not need anyone’s authorization to access them. Their long-term residence on plaintiffs’ hard drives places them outside of § 2510’s definition of “electronic storage” and Title II’s protection. Even if they were in “electronic storage,” DoubleClick is authorized to access its own communications.

Plaintiffs have offered no explanation as to how the Doubleclick-affiliated Web sites could have played such a central role in the information collected and not have authorized DoubleClick’s access.

Therefore, we find that DoubleClick-affiliated Web sites consented to Doubleclick’s access of plaintiffs’ communications to them. DoubleClick’s practices and consumers privacy concerns with them are unknown to Congress. Indeed, Congress is currently considering legislation that specifically recognizes the online harvesting of user information.

For the foregoing reasons, DoubleClick’s motion to dismiss is granted.

IT IS SO ORDERED.

Case Questions

1. How did the court determine that the Web sites authorized DoubleClick to access plaintiffs’ electronic communications?
2. Why did the court decide the cookies placed on users’ hard drives were not in temporary “electronic storage”?
3. How can DoubleClick’s practice in placing the cookies be justified ethically?

(Postscript: After this decision, the plaintiffs filed appeals in the federal Court of Appeals and the California Superior Court. In March 2002, pending the outcome of these appeals, a settlement was reached whereby DoubleClick agreed to pay $1.8 million in damages to the plaintiffs. In August 2002, in order to end an investigation spearheaded by New York’s attorney general Eliot Spitzer and ten other states to determine if DoubleClick created consumer profiles unlawfully, DoubleClick agreed to pay $450,000 in damages, to better disclose how it tracks consumers online, to allow consumers to access the profiles created about them, and to allow for an independent audit of its privacy policies for several years.)
Title III (U.S.C. §§ 3121-3127): The Pen Register Act

Title III applies to wiretaps, pen registers, and trap and trace devices. Recall that a pen register records phone numbers dialed from another phone. A trap and trace device records the phone numbers where incoming calls originated. Before a government agency can use either, Title III requires that it obtain a court order which will only be granted if the information sought is relevant to an ongoing criminal investigation. Also, note that if the facts indicate the monitoring was excessive, a court could rule it was more like a wiretap than a pen register for which a search warrant rather than a court order would be required. The result could render any evidence obtained to be in violation of the Fourth Amendment and therefore inadmissible.

Keep in mind that the USA Patriot Act amended Title III of the ECPA (and at least fifteen other federal statutes) by broadening the surveillance powers of the federal government to combat threats of terrorism, some argue at the expense of the rights to privacy of innocent individuals or individuals suspected of nonterrorist crimes for which they are entitled to more Fourth Amendment protection. These powers extend to monitoring e-mail and computer usage. You will study the effect of the USA Patriot Act in more detail in Chapters 12 and 13.

Privacy and Spam ("Unsolicited Commercial E-mail")

No doubt you have been online when an unsolicited and perhaps unwanted (spam) ad appears on your screen. Estimates are that each of us will receive a spam over two thousand times this year and by 2006, over four thousand times. As you already learned, the Telephone Consumer Protection Act, state laws, and the FTC proposed initiative give us the right not to be called by a telemarketing company. To date, no such right applies to spam and, for those who have not given permission to receive these ads, they have become just as much an annoyance as those unwanted telemarketing calls.

Efforts by members of Congress to pass federal antispam laws have not been successful. The position of the FTC has consistently been that self-regulation (more discussion later) rather than federal legislation is the most effective way to control spam. More than half the states disagree with the FTC and have adopted antispam laws or have imposed strict requirements and controls for its use. It should also be mentioned that international laws on spam differ from country to country. Austria, Denmark, and Italy require consumers to opt in; England, Canada, and France require them to opt out before receiving spams.

A state case involving spam is State of Washington v. Heckel, 24 P. 3d 404 [(Supreme Court of Washington, 2001, certiorari denied, 122 S. Ct. 467 (2001))], where a state act prohibited sending spam that "misrepresents or disguises the message’s point of origin or transmission path or uses a misleading subject line." It also
prohibited a spammer from failing to provide an e-mail address to which the recipient of the spam could respond. The act was challenged on the basis that it was discriminatory against out-of-state businesses and therefore imposed a burden on interstate commerce in violation of the dormant Commerce Clause of the U.S. Constitution. The dormant clause that applies to a state law where there is no applicable federal law limits and, in some cases, prohibits the power states have to pass laws to regulate interstate commerce.

The court in *Heckel* held that the state antispam law was not discriminatory on its face because it applied equally to intrastate as well as interstate businesses. The court also held that the benefits of the act outweighed any burdens imposed. It would reduce the Internet traffic jam caused by mass spam, protect the owners of domain names, and help reduce the Internet access costs for unwanted e-mail paid for by its recipients be they businesses or individuals. In essence, the court said the “only burden the Act places on spammers is the requirement of truthfulness, a requirement that does not burden commerce at all but actually facilitates it by eliminating fraud and deception.”

Thus we can see that unless there is a state antispam law or you have taken steps to prevent spam by opting out (consumers have complained that clicking “Remove me” or similar buttons has been ineffective) or installing blocking software, there is very little you can do regarding spam. Note, in the past five years, the FTC reports having received over 250,000 spam complaints resulting in over thirty enforcement actions. Why has spam become so prevalent a marketing and advertising tool? E-businesses maintain that spam is a relatively inexpensive method to reach huge numbers of prospective customers and is very profitable (2002 retail sales online were estimated to be over $72 billion, a 41 percent increase over 2001). Amazon estimated its sales for 2002 to be $850 million. It would be difficult to determine the effect of spam on those figures. Again, for many, the spam serves only to annoy, invade privacy, and create a kind of online “traffic jam.”

You are probably aware where these e-commerce companies get our names and other personal information about us for spamming and other purposes. As we indicated in the introduction to this chapter, and as we discovered in the *DoubleClick* case, every time we visit a Web site we leave a “fingerprint” of information about ourselves in the form of a cookie. Not only is personal information about us stored on the cookie, but also other information such as our buying habits and preferences. E-commerce businesses are willing to pay for this valuable information. Thus the gathering of such data has evolved into big business for many companies specializing in the sale of it in the form of lists. This has led to what is called *online profiling*. Privacy concerns arise because these lists and profiles are sold without our consent or knowledge and are often the catalyst for spam. E-businesses argue that these profiles are useful in targeting interested consumers for receiving customized information about their products or services, special events, and other matters of interest. It should be obvious that as long as the profiling process and the resultant solicitations meet the requirements of the law, they will likely be protected as exercises of free speech or enterprise.
One of the most significant industry self-regulation initiatives recommended by the FTC for Web sites that collect personal identifiable information (PII) is that their online privacy policies be drafted in accordance with the **fair information practices** (see Figure 9.2) (first suggested in 1973 by the Department of Health Education and Welfare's Advisory Committee on Automated Data Systems and advocated by the FTC in its Reports to Congress). Keep in mind, there are a number of concerned consumer watchdog groups such as the Electronic Privacy Information Center (EPIC), Center for Democracy and Technology, the Electronic Frontier Foundation, and the Privacy Rights Clearinghouse, whose agendas focus on monitoring and safeguarding personal privacy online and who also recommend policies based on the practices (see Figure 9.3).

**Is Self-Regulation Working?**

The FTC conducted a survey in 2000 consisting of a sample random group of 335 Web sites (“Random Sample”) and 100 of the busiest sites. The results indicated that nearly 100 percent of the sites collected some type of PII and posted a privacy policy, but only 50 percent met the basic **Notice** and **Choice** requirements of the FIP.

The FTC is not completely convinced that self-regulation is the answer to controlling spam but will allow it to continue focusing its efforts on continuing to apply and enforce its regulations against deceptive and fraudulent spams and inadequate privacy policies. It did so in the following case involving spam. In *FTC v. GM Funding, Inc.*, *Global Mortgage Inc.*, et al., SACV 02-1026 DOC—U.S. District Court, CA (2002), the FTC charged the defendant with “spoofing,” which was described as disguising an e-mail to make it appear it was mailed from an address different from the one from which it was actually mailed without the permission of the user of the actual “spoofed” address. In this case, spams were sent in the name of and along with the trademarks of well-known financial institutions that offered, among other services, mortgages and other financial services. Those “spoofed” included Prudential, Radian Corporation, and the Fannie Mae Corporation.

The spams requested personal financial information from consumers including income and credit ratings under the pretense it would be used to help the consumers obtain mortgages. Attempts by the consumers to stop the spam failed. In fact, the information was sent to an IP address registered to the defendant, who transferred it to another defendant who could then solicit the consumers about obtaining mortgages.

The FTC charged the defendants with unfair and deceptive practices under Section 5 of the FTC Act and with violating Section 521 of the GLB Act, 15 U.S.C. § 6821, which prohibited obtaining customer personal financial information of a financial institution by false, fictitious, or fraudulent statements. The court agreed and issued an injunction preventing these practices in the future. *(Note: The defendants did not admit guilt but opted to avoid a trial by agreeing to the injunction.)*
FIGURE 9.2   FTC's Fair Information Practices

Web sites that collect personal identifying information (PII) about or from consumers should comply with the following:

- **Notice:** Indicate information collection practices before collection.
- **Choice:** Inform how information is to be used along with opportunities to deny or grant permission for collection of PII.
- **Access:** Allow access to information already collected to determine and correct, if necessary, inaccurate or incomplete information.
- **Security:** Make sure information is protected from unauthorized use, access, or disclosure.
- **Enforcement:** Implement procedures to subject themselves to outside monitoring to ensure compliance with appropriate sanctions and remedies for violations.

FIGURE 9.3   Industry Attempts to Address Spam and Related Privacy Issues

- **World Wide Web Consortium (W3C), Platform for Privacy Preferences (P3P):** A leader in developing technical specifications for the Web's infrastructure in order to further and enhance its growth and operation. Over 450 member Web sites post their privacy policies automatically, making them viewable by visitors who may then choose what information they will or will not allow to be collected. (See http://www.w3.org.)
- **TRUSTe:** An independent, nonprofit Internet privacy organization sponsored by AOL, Microsoft, and others, comprised of more than six hundred member companies. Its major function is to monitor the sites of its members making sure their information practices are fair and sensitive to privacy rights. Members are also required to inform users about how personal information about them is used and to establish oversight and consumer complaint procedures. Those in compliance receive a trustmark (a type of online "seal of approval"). (See http://www.truste.org.)
- **Network Advertising Initiative:** Its members include DoubleClick, Avenue A, and other online providers of advertising services and products, all of whom are committed to providing the privacy protections associated with the fair information practices (FIP). (See http://www.networkadvertising.org.)
- **Direct Marketing Association (DMA):** Provides information and guidance to its members. In 2002, approved and mandated a set of online information guidelines for its members who operated Web sites and engaged in bulk e-mail solicitations. (See http://www.the-dma.org/library/guidelines/onlineguidelines.shtml.)
- **Netiquette** is an unofficial attempt at self-regulation by businesses engaged in cyberspace. It proscribes a kind of ethical code of etiquette to be followed when dealing with customers or users online. Generally, it seeks to require courtesy and respect online. It also seeks to ensure that bandwidths are not clogged.
For insight as to how federal courts have treated other cases involving spam, consider the following two cases. In the first case, *Cyber Promotions v. America Online, Inc.*, the court had to balance First Amendment guarantees of freedom of speech associated with commercial speech, against the rights of the individual to be free from what they perceive to be an annoying interference with privacy rights.

In the second case, *CompuServe, Inc., v. Cyber Promotions*, the court was asked to apply the common law theory of trespass to the sending and receiving of electronic signals. The judges in both cases categorized the issues presented for decision as “novel.”

---

**Cyber Promotions, Inc., v. America Online, Inc.**  

**Facts**

The plaintiff, Cyber Promotions, is a private company incorporated in Pennsylvania. It provides advertising services for companies and individuals. One of its business activities is sending unsolicited e-mail advertisements through the Internet to America Online (AOL) subscribers.

AOL is a private company offering computer online services. Its members pay prescribed fees for use of AOL resources, access to AOL, and access and use of AOL’s e-mail system and connection to the Internet.

AOL’s computer servers have a finite, though expandable, capacity to handle e-mail. It allows its subscribers to send and receive e-mail to and from AOL, as well as non-AOL, members. Under either scenario, these services require the use of AOL’s computer hardware and software. AOL subscribers pay a monthly service fee, and AOL is responsible for processing all of this information, including the e-mail.

In a letter dated January 26, 1996, AOL advised Cyber that it was upset with Cyber’s dissemination of unsolicited e-mail to AOL subscribers. Apparently these advertisements continued despite the letter. AOL subsequently sent a number of “bombs” to Cyber’s Internet service providers (ISPs). Cyber has stated that the “bombs” occurred when AOL gathered all unsolicited e-mail sent by Cyber to undeliverable AOL addresses, altered their return, and then sent the altered e-mail in a bulk transmission to Cyber’s ISPs in order to disable the ISPs. Cyber filed suit first, alleging that as a result of the bombing, two of its ISPs terminated their relationship with Cyber, and a third ISP has refused to enter into a contract with Cyber. The complaint asserts claims under the Computer and Fraud Abuse Act, and state law claims such as intentional interference with contractual relations.

Two weeks later, AOL filed a complaint against Cyber for, *inter alia*, service and trade name infringement and violations of the Virginia Consumer Protection Act and the Electronic Communications Privacy Act. One month later, Cyber added a declaratory judgment claim seeking a “declaration that [it] has the right to send to AOL members, via the Internet, unsolicited e-mail advertisements.” AOL has vehemently argued throughout the brief history of these suits that Cyber has no right to send literally millions of e-mail mes-
sages each day to AOL's Internet servers, free of charge, resulting in the overload of the e-mail servers. Cyber argues, however, that by providing these services, AOL has opened up this domain for public use, and as such performs a public function open to the public.

The trial judge consolidated the two cases because they arise from the same nucleus of operative facts. AOL motioned for partial summary judgment on Cyber's First Amendment claim.

Judicial Opinion *(Memorandum Opinion and Order, District Judge Weiner)*

These cases present the novel issue of whether, under the First Amendment to the United States Constitution, one private company has the unfettered right to send unsolicited e-mail advertisements to subscribers of another private online company over the Internet and whether the private online company has the right to block the e-mail advertisements from reaching its members. The question is important because while the Internet provides the opportunity to disseminate vast amounts of information, the Internet does not, at least at the present time, have any means to police the dissemination of that information.

Under Federal Rule of Civil Procedure 56(c), summary judgment may be granted when, 'after considering the record of evidence in the light most favorable to the non-moving party, no genuine issue of material fact exists and the moving party is entitled to judgment as a matter of law.' In its motion ... AOL contends that Cyber has no First Amendment right to send unsolicited e-mail ... because AOL is not a state actor.

The First Amendment to the United States Constitution states that 'Congress shall make no law ... abridging the freedom of speech, or of the press.' Only recently the Supreme Court has stated that 'the guarantees of free speech ... guard only against the encroachment by the government and erect no shield against merely private conduct.' In the case sub judice, the parties have stipulated that AOL is a private online company that is not owned in whole or in part by the government. They have also stipulated that there has been no government involvement in AOL's business decision to institute ... a block directed to Internet e-mail sent by Cyber to AOL members or subscribers.

Despite these stipulations, Cyber argues that AOL's conduct has the character of state action. As a general matter, private action can only be considered state action when 'there is a sufficiently close nexus between the State and the challenged action [of the private entity] so that the action of the latter may be fairly treated as that of the state itself.'

Pursuant to the Court's directive, the parties have stipulated to the following facts: 'No single entity—academic, corporate, governmental, or non-profit—administers the Internet. Although the Internet is accessible to all persons, ... the constituent parts ... are owned and managed by private entities.'

In sum, we find that since AOL is not a state actor and there has been no state action by AOL's activities under any of the ... tests for state action enunciated by our Court, Cyber has no right under the First Amendment to send unsolicited e-mail to AOL's members. The motion of America Online, Inc., for partial summary judgment on First Amendment issues is GRANTED.

IT IS SO ORDERED.
Case Questions

1. How did Cyber's spamming activities interfere with AOL's contractual relations?
2. What provisions of the ECPA do you believe were violated by Cyber?
3. Is it ethical to allow an ISP to block all spam messages, especially in cases where a subscriber does not object to receiving them?

CompuServe, Inc., v. Cyber Promotions

Facts

CompuServe is one of the major national commercial online computer services. In addition to its other services, CompuServe also provides its subscribers with a link to the much larger resources of the Internet. This allows its subscribers to send and receive electronic messages, known as "e-mail," by the Internet. CompuServe subscribers use CompuServe's domain name together with their own unique alphanumeric identifier to form a distinctive e-mailing address. E-mail sent to CompuServe subscribers is processed and stored on CompuServe’s proprietary computer equipment and subscribers electronically retrieve those messages.

Defendants, Cyber Promotions, Inc., and its president Sanford Wallace, are in the business of sending unsolicited e-mail advertisements on behalf of themselves and their clients to hundreds of thousands of Internet users, many of whom are CompuServe subscribers threatening to discontinue service unless CompuServe prohibits mass mailers from using its equipment. CompuServe receives no payment from the mass mailers and asserts that the volume of e-mail messages generated places a significant burden on its equipment, which has finite processing and storage capacity. Subscribers pay for their access to CompuServe’s services in increments of time, and thus the processing of unsolicited e-mail costs them money.

CompuServe notified defendants that they are prohibited from using its computer equipment to process and store the unsolicited e-mail. In an effort to shield its equipment from defendants' bulk e-mail, CompuServe has implemented software programs designed to screen out messages and block their receipt. Allegedly, defendants have been able to continue sending messages to CompuServe’s equipment in spite of CompuServe’s protests and protective efforts.

CompuServe brought suit, alleging the defendants have trespassed on their personal property. CompuServe motioned this court for a preliminary injunction to prevent defendants from sending them unsolicited advertisements. Defendants assert that they possess the right to continue to send these communications under the First Amendment constitutional guarantee of free speech.
This case presents novel issues regarding the commercial use of the Internet. [The court first addressed CompuServe’s request for a Temporary Restraining Order in which it enjoined defendants] from performing any of the acts . . . described during the pendency of this litigation.

CompuServe predicates . . . its motion for a preliminary injunction on the common law theory of trespass to personal property or to chattels, asserting that defendants’ continued transmission of electronic messages to its computer equipment constitutes an actionable tort.

Trespass to chattels has evolved from its original common law application, concerning primarily the asportation of another’s tangible property, to include the unauthorized use of personal property:

Its chief importance now is that there may be recovery . . . for interferences with the possession of chattels which are not sufficiently important to be classed as conversion, and so to compel the defendant to pay the full value of the thing with which he has interfered. Trespass to chattels survives today, in other words, largely as a little brother of conversion.

While authority under Ohio law respecting an action for trespass to chattels is extremely meager, it appears to be an actionable tort. Both plaintiff and defendant cite the Restatement (Second) of Torts to support their respective positions. In determining a question unanswered by state law, it is appropriate for this Court to consider such sources as the Restatement of the law and decisions of other jurisdictions.

The Restatement § 217 (b) states that a trespass to chattels may be committed by intentionally using or intermeddling with the chattel in possession of another. Electronic signals generated and sent by computer have been held to be sufficiently physically tangible to support a trespass cause of action in California. [The] Indiana Supreme Court recognized in dicta that a hacker’s unauthorized access to a computer was more in the nature of trespass than criminal conversion. [A Washington state court held] computer hacking as the criminal offense of ‘computer trespass’ under Washington law. It is undisputed that plaintiff has a possessory interest in its computer systems. Further, defendants’ contact with plaintiff’s computers is clearly intentional.

Under Restatement § 252, the owner of personal property can create a privilege in the would-be trespasser by granting consent to use the property. Defendants argue [just this]. Their argument is analogous to the argument that because an establishment invites the public to enter its property for business purposes, it cannot later restrict . . . access . . ., a proposition which is erroneous under Ohio law.

In response to the trespass claim, defendants [also] argue that they have the right to continue to send unsolicited . . . under the First Amendment. The United States Supreme Court has recognized that “the constitutional guarantee of free speech is a guarantee only against abridgement by the government.” In the present action, CompuServe is a private company. Defendants’ . . . use is an actionable trespass to plaintiff’s chattel. The First Amendment to the United States Constitution provides no defense for such conduct.

Plaintiff has demonstrated a likelihood of success on the merits . . . [and] has shown that it will suffer irreparable harm without the grant of a preliminary injunction. Based on the
foregoing, plaintiff's motion for a preliminary injunction is GRANTED. The temporary restraining order . . . is hereby extended in duration until final judgment is entered in this case.

IT IS SO ORDERED.

Case Questions

1. What "irreparable harm" will the plaintiff suffer without the injunction?
2. Do you agree that electronic signals should be classified as physically tangible personal property?
3. How can a company ethically justify engaging in a business that appears to create an annoyance and invasion of privacy?

The day after the AOL decision, Sanford Wallace, the so-called spam king, entered into a settlement agreement with AOL. The agreement provided that AOL be allowed to install what it calls "PreferredMail." This allowed AOL subscribers the option to receive or block unsolicited e-mail advertisements such as those offered by companies like Cyber Promotions. Both sides considered this settlement a victory. However, you should recognize that this settlement applied only to Cyber Promotions and AOL.

Workplace Privacy

Employees' inappropriate e-mail and usage of computers owned and maintained by employers continue to provide a fertile environment for privacy issues and litigation. From the employer's perspective, employee workplace privacy rights, whether they exist under the Fourth Amendment search and seizure provisions, other statutes, or common law torts, are overcome by the employer's vested economic interest in ensuring employee productivity and protection of the employer from potential liability for harassment, discrimination, obscenity, and defamation as well as protection of trademark, trade secret, and other proprietary interest violations that could result from inappropriate and unsupervised employee computer usage.

This right to search an employee's office, desk, and files was recognized in O'Connor v. Ortega, 480 U.S. 709 (1987), where the U.S. Supreme Court held that a public or government employer could do so provided the search was "reasonable under all circumstances." The Court stated that the employee's legitimate expectation of privacy had to be "balanced against the government's need for supervision, control and the efficient operation of the workplace." As we will discover, the rationale used for the decision in Ortega is the similar to that used by other courts in workplace privacy cases involving employees in the private sector.
How Common Is the Problem of Employee Inappropriate Computer Use?

In 1999, a study conducted by the Elron Software Corporation determined that over 85 percent of the employees responding indicated they used employer e-mail systems for personal use, and over 60 percent indicated they visited adult Web sites with more than 50 percent receiving inappropriate e-mails. Although the law has yet to be settled in this area and there are virtually no U.S. Supreme Court cases in this area, there are some trends or precedents that provide possible guidance and predictability concerning employer liability.

Employer liability appears to be greatly diminished, but not eliminated, where the employer has developed a clear and written computer-monitoring and usage policy communicated on a regular basis to all employees. Obtaining employee consent to the monitoring is also a mitigating factor for liability (also under the ECPA's exceptions). Keep in mind that the employer's rights are not limitless even with a valid policy and with employee consent to monitoring. For example, an employer would have difficulty justifying around the clock (“24/7”) monitoring in the absence of a business-related reason (Sanders v. Bosch, 38 F. 3d 736 [1994]). The same could be true where the employer’s monitoring policy only applied to business messages and personal messages were intercepted and accessed (Watkins v. L.M. Berry & Co., 704 F.2d 577 [11th Cir. 1983]).

How prevalent are such policies? A workplace privacy survey in 2000 conducted by the Society for Human Resource Management and West Group indicated that 70 percent of the 722 human resource managers reported having computer and e-mail monitoring policies and 94 percent reported the policies were communicated to their employees. In companies that have policies, employees experience difficulty in proving that they enjoyed a reasonable expectation of privacy in their computer use and especially their e-mail. Recall our earlier discussion in the Katz case and of the tort of intrusion upon seclusion where the element of a reasonable expectation of privacy was critical to proving an invasion of privacy rights. This element continues to be one of the most critical discussion points in many of the cases decided in this area. Without such a policy, the employer can be exposed to liability.

In Nardinelli et al., v. Chevron, No.945302, Superior Court, CA (1995), Chevron had an anti-harassment policy but none for computer usage or monitoring. Nardinelli and other employees sued Chevron, claiming they were sexually harassed by e-mails sent to them by other employees that offered 25 reasons why beer was better than women. Chevron settled out of court with the employees for $2.2 million.

In a more recent case, an employer had no monitoring policy regarding its online bulletin board outside the workplace on which employees could post messages. Defendant’s employees posted harassing comments on the bulletin board about the plaintiff. Although the employer was informed about them, it did nothing, believing the bulletin was not outside the workplace. The court took a different view, ruling that even though the bulletin board did not have a physical presence in the workplace, it was close enough so harassment posted on it would be considered to have occurred in the workplace. Further, the court made a point of the fact that once the employer
knew of the comments, it had a legal duty to stop them. The plaintiffs in that case were awarded $1.7 million in damages (see Blakey v. Continental Airlines, 751 A. 2d 538 (N.J. 2000)).

In the following case, an employer promised it would neither read employee e-mail nor terminate or reprimand an employee based on the content of the e-mail. The employer did intercept the employee’s e-mail, found it unprofessional and inappropriate, and fired him.

Michael A. Smyth v. Pillsbury Company
914 F. Supp. 97 (E.D. Pa., 1996)

Facts

Plaintiff, an at-will employee, received certain e-mail communications from his supervisor over defendant’s e-mail system on his computer at home. At some later date, contrary to the assurances of confidentiality made by defendant, defendant intercepted plaintiff’s e-mail messages. The messages concerned statements about the sales management and contained threats to “kill the backstabbing bastards.” They also referred to the planned holiday party as the “Jim Jones Koolaid affair.”

As a result, plaintiff is terminated for transmitting what the defendant deemed to be inappropriate and unprofessional comments over defendant’s e-mail system.

Judicial Opinion (Judge Weiner)

As a general rule, Pennsylvania law does not provide a common law cause of action for the wrongful discharge of an at-will employee such as the plaintiff. An employer “may discharge an employee at-will with or without cause, at pleasure, unless restrained by some contract.”

Henry v. Pittsburgh & Lake Erie Railroad Co., 139 Pa. 289, 21 A. 157 (1891). However, in the most limited circumstances, exceptions have been recognized where discharge of an at-will employee threatens or violates a clear mandate of public policy. This public policy exception is an especially narrow one. To date, the Pennsylvania Superior Court has only recognized three such exceptions. First, an employee may not be fired for serving on jury duty.

Second, an employer may not deny employment to a person with a prior conviction.

And finally, an employee may not be fired for reporting violations of federal regulations to the Nuclear Regulatory Commission.

As evidenced above, a public policy exception must be clearly defined. Plaintiff claims that his termination was a violation of public policy, which precludes an employer from terminating an employee in violation of the employee’s right to privacy as embodied in Pennsylvania common law. In support for this proposition, plaintiff directs our attention
to a decision by our Court of Appeals in *Borse v. Piece Goods Shop, Inc.*, 963 F. 2d 611 (3rd Cir. 1992). In *Borse*, the plaintiff sued her employer alleging wrongful discharge as a result of her refusal to submit to urinalysis screening and personal property searches at her workplace pursuant to employer's drug and alcohol policy. After rejecting plaintiff's argument that the employer's drug and alcohol program violated public policy embodied in the United States and Pennsylvania Constitutions, our Court of Appeals stated "our review of Pennsylvania law reveals other evidence of public policy that may, under certain circumstances, give rise to a wrongful discharge action related to urinalysis or to personal property searches. Specifically, we refer to Pennsylvania common law regarding invasion of privacy." One of the torts Pennsylvania recognizes as encompassing an action for invasion of privacy is the tort of "intrusion upon seclusion." The Restatement (Second) of Torts defines the tort as follows:

One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Liability only attaches when the intrusion is "substantial and would be highly offensive to the 'ordinary reasonable person.'" *Borse*, 963 F. 2d at 621. Although the Court of Appeals in *Borse* observed that "the Pennsylvania courts have not had occasion to consider whether a discharge related to an employer's tortious invasion of an employee's privacy violates public policy," the Court of Appeals predicted that in any claim where the employees claimed that his discharge related to an invasion of his privacy, "the Pennsylvania Supreme Court would examine the facts and circumstances surrounding the alleged invasion of privacy. If the court determined that the discharge was related to a substantial and highly offensive invasion of the employee's privacy, we believe that it would conclude that the discharge violated public policy." In determining whether an alleged invasion of privacy is substantial and highly offensive to a reasonable person, Pennsylvania would adopt a balancing test which balances the employee's privacy interest against the employer's interest in maintaining a drug-free workplace. Because the Court of Appeals in *Borse* could envision at least two ways in which an employer's drug and alcohol program might violate the public policy protecting individuals from tortious invasion of privacy, the Court vacated the district court's order dismissing the plaintiff's complaint and remanded the case to the district court with directions to grant Borse leave to amend the complaint to allege how the defendant's drug and alcohol program violates her right to privacy.

Applying the Restatement definition of the tort of intrusion upon seclusion to the facts and circumstances of the case *sub judice*, we find that plaintiff has failed to state a claim upon which relief can be granted. In the first instance, unlike urinalysis and personal property searches, we do not find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system, notwithstanding any assurances that management would not intercept such communications. Once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system, which was apparently utilized by the entire company, any reasonable expectation of privacy was lost. Significantly, the defendant did not require plaintiff, as in the case of a urinalysis or personal property search, to disclose
any personal information about him. Rather, plaintiff voluntarily communicated the alleged unprofessional comments over the company e-mail system. We find no privacy interests in such communications.

In the second instance, even if we found that an employee had a reasonable expectation of privacy in the contents of his e-mail communications over the company e-mail system, we do not find that a reasonable person would consider the defendant’s interception of these communications to be a substantial and highly offensive invasion of privacy. Again, we note that by intercepting such communications, the company is not requiring the employee to disclose any personal information about him or invading the employee’s person or personal effects. Moreover, the company’s interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments.

In sum, we find that the defendant’s actions did not tortiously invade the plaintiff’s privacy and, therefore, did not violate public policy. As a result, the motion to dismiss is granted.

IT IS SO ORDERED.

Case Questions

1. Do you think Smyth should have been given a warning he would be terminated the next time he made these kinds of comments? Were they that serious?
2. How can a court justify the “chilling effect” employer interception of employee e-mail appears to have on an employee’s freedom of speech?
3. Was it ethical for the employer to break the promise not to read employee e-mail or terminate or reprimand an employee based on the content of the e-mail?

In a more recent case, McLaren v. Microsoft, Case No. 05-97-00824, 1999 Tex. App. LEXIS 4103 (Tex. Ct. of App. 1999), McLaren was fired after his employer, Microsoft, broke into and accessed his personal folders that were protected by a password known only to McLaren and discovered files that contained evidence of sexual harassment. McLaren argued that because Microsoft allowed him to have a password for his personal folders, a reasonable expectation of privacy was created and Microsoft’s actions resulted in violations of the Fourth Amendment, the tort of intrusion upon seclusion, and an invasion of privacy. However, the court decided for Microsoft, reasoning that because the e-mails had to first travel through various points in Microsoft’s e-mail system before reaching McLaren’s folder, Microsoft could have accessed them before they reached his folder, thereby eliminating any reasonable expectation of privacy. The court offered reasoning similar to that in Smyth, providing the following guidelines for similar future cases:
• Microsoft's actions would not be considered highly offensive to a reasonable person.
• The folders were business related and not personal.
• The e-mails belonged to Microsoft and the employees.
• Microsoft had a right to prevent inappropriate and unprofessional comments or potential illegal activities such as sexual harassment and this right outweighed any privacy rights enjoyed by McLaren.

Smyth and McLaren serve notice to employees that they should expect little or no privacy in the workplace. Particular attention should be paid to the similar reasoning employed by both courts. It provides some guidelines and predictability for cases of these types. However, remember that the law is still unsettled in this area so other courts could decide differently in cases involving similar facts. A Massachusetts trial court appears to have done exactly that in Restuccia v. Burk Technology, 5 Mass. L. Rptr, No. 31, 712 (Middlesex Superior Court, 1996), where the employer suspected the employee of sending inappropriate personal e-mails through the employer's e-mail system. The employer allowed the employees to have personal passwords, send personal e-mails, and never told them their e-mails could be accessed. In effect there was no monitoring policy. Without offering reasoning, the court believed there existed a question of fact to be decided by a jury as to whether the employees enjoyed a reasonable expectation of privacy that was violated by the employer's intrusion (upon seclusion) resulting in an invasion of privacy.

Impact of the ECPA on Workplace Privacy

Recall that Title I of the ECPA prohibits the unauthorized interception of an electronic communication including e-mail in transmission and Title II prohibits accessing and disclosing such communications if they are in storage. As mentioned earlier, both titles provide for exceptions.

In the following case, the plaintiff brought claims alleging violations of the ECPA and the Railway Labor Act for wrongful interference with union organizing activities. The case was originally tried in federal district court and was appealed to the federal court of appeals twice. The second appeal is presented here.

Robert Konop v. Hawaiian Airlines
302 F.3d 868 (9th Cir. 2002)

Facts

Konop was a pilot for Hawaiian Airlines (HA) and operated a secure Web site accessible only by a password he would assign to users. He also created a list of “users.” During union negotiations, he posted messages critical of his employer, its officers, and the union
to which he belonged. He also urged employees to seek alternative union representation. Davis, HA's vice president, believed Konop was posting false allegations on his Web site and enlisted the aid of Wong, another pilot who had a password but had never logged on to the Web site. Davis used Wong's name and password to access the Web site and discovered the comments. He disclosed them to other officers of the company and to the union. Konop files suit in federal district court claiming these actions violated his privacy under Title I of the ECPA (referred to in the case as the Wiretap Act) and Title II of the ECPA (referred to in the case as the Stored Communications Act) prohibitions against interception of electronic communications, alleging that HA viewed his secured Web site and disclosed the contents of the messages he had posted. Further, he alleged the actions resulted in unauthorized surveillance of union activities prohibited by the Railway Labor Act (RLA). The district court ruled against Konop as to his claims under Title I, holding there was no "interception" of the message by Davis because it occurred when the message was "in storage" and not when it was "in transmission" as required by Title I.

The district court also ruled against Konop in his Title II claim holding that the actions were covered by an exception to Title II that allows access "without authority" where the "conduct is authorized by a user of that service with respect to a communication of or intended for that user." The exception required that a "user" actually use or access the Web site, not merely possess a password to do so. Wong had never accessed the Web site and without evidence of that fact, the court ruled both Wong and Davis were users and therefore there was no Title II violation. The court did find a violation of the RLA had occurred. In the first appeal to this court in January 2001, the court reversed the decision of the district court as to the ECPA claims, ruling there were violations of both Title I and II. It affirmed the decision regarding the RLA (236 F.3d 1035 (9th Cir. 2001). HA filed a petition for a rehearing that became moot when the court withdrew its January 2001 opinion leading to this appeal.

**Judicial Opinion (Circuit Judge Boochever)**

For a website such as Konop's to be "intercepted in violation of the Wiretap Act (Title I of the ECPA), it must be acquired during transmission not while it is in storage. This conclusion is consistent with the ordinary meaning of "intercept" which is to "stop, seize, or intercept in progress of course before arrival." (Webster's Dictionary) More importantly, it is consistent with the structure of the ECPA, which created the Stored Communications Act (SCA) for the express purpose of addressing "access to stored ... electronic communications and transactional records." The level of protection provided stored communications under the SCA is considerably less than that provided under the Wiretap Act. The SCA details the procedures law enforcement must follow to access contents of stored communications and these are less burdensome than those required to obtain a wiretap order under the Wiretap Act. Thus, if Konop's position were correct and acquisition of a stored electronic communication were an interception under the Wiretap Act, the government would have to comply with the more burdensome and restrictive procedures under the Wiretap Act to do exactly what Congress intended it to do under the less burdensome procedures of the SCA. Congress could not have intended that result. We conclude that for a website such as Konop's to be "intercepted" in violation of the Wiretap Act, the electronic communication must be acquired during transmission and not while it is in storage.
Davis' conduct did not constitute an "interception of an electronic communication" in violation of the Wiretap Act. We affirm the district court's grant of a summary judgment against Konop on his wiretap claim.

Konop also argues that by viewing his secure website, Davis accessed a stored electronic communication without authorization in violation of the SCA (Title II of the ECPA). The parties agree that the relevant "electronic communication service" is Konop's website, and that the website was in electronic storage. Davis' conduct constituted "access without authorization" to "a facility through which an electronic communication is provided."

We address only the narrow question of whether the district court properly found Hawaiian Airlines exempt from liability under § 2701 (c) (2) which allows a person to authorize a third party's access to an electronic communication if the person is (1) a "user" of the "service" and (2) the communication is "of or intended for that user." The district court concluded that Wong had the authority under § 2701 to consent to Davis' use of the website because Konop put them on the list of eligible users. As intended recipients of wire and electronic communications, they were allowed to authorize third parties to access those e-mail communications. The district court did not make any finding on whether Wong actually used Konop's website. We cannot find any evidence that Wong ever used Konop's website and we must assume that he was not a "user" under § 2701 (c) (2) at the time he authorized Davis to view it. We therefore reverse the district court's summary judgment to Hawaiian on Konop's CA claim.

For the foregoing reasons, we affirm the district court's judgment with respect to Konop's Wiretap Act claims (and those under the RLA) and reverse the district court's judgment on Konop's claims under the SCA.

AFFIRMED IN PART, REVERSED IN PART, AND REMANDED.

Case Questions

1. Would the decision in this case have been different if Konop's Web site was accessible by a nonprotected password?
2. What facts were critical to the court of appeals' determination that Davis had violated the Stored Communications Act (Title II of the ECPA)?
3. How do the facts in this case differ from those in Smyth?

CONCLUSION

From our discussion, it should be obvious that employee privacy rights in the workplace are virtually nonexistent. However, in order to balance the interests of the employer with those of the employee, and create a workplace environment characterized by productivity, high morale, and mutual respect, all employers would be well
advised to develop and implement a written computer usage policy, including a right
to monitor, applicable to company-owned computers and electronic communications
whether used on the business premises or at another location. From a legal stand­
point, the policy should stress that employees have no reasonable expectation of pri­
vacy in company-owned property. The policy should be developed in consultation
with the company attorney and other relevant individuals and departments including
the employees or their representatives. Proper consideration should be given to the
company culture. Figure 9.3 suggests the elements of a computer usage policy that a
court could look to in employee privacy cases. Also, keep in mind that proper imple­
mentation of the policy is important. Courts will look to see if:

- Appropriate training programs regarding company requirements for computer
  usage are provided.
- The policy is in writing and conspicuously displayed in company employee lit­
  erature (manuals, etc.).
- Every employee executes a written acknowledgment that they have received.
- Employees are reminded of the policy yearly.

Keep in mind that the policies listed in Figure 9.4 are not yet mandatory either under
federal or state law. There is no guarantee that even with a policy the employer will be

**FIGURE 9.4** Suggested Elements of an Employee Workplace
Computer Use Policy

- Indicate the reasons for the policy.
- Indicate that employees should expect no privacy in company-owned property.
  *Apply the policy to all employees including the CEO.*
- Inform employees that computers issued to them are to be used for business
  purposes only (delineate any allowable personal uses).
- Indicate the nature and extent of computer monitoring, that it can be done at
  any time without notice, and describe the use of any related software or other
  methods for that purpose. Indicate the nature and extent of the impact imposed
  on the company by the USA Patriot Act.
- Inform employees that all communications, data, and documents stored in
  computers are confidential unless made public by the company. If relevant,
  inform employees on the methods to be used in handling such information.
- Zero tolerance will apply to offensive, harassing, or discriminating communica­
  tions or e-mails and visits to inappropriate Web sites.
- Prohibit employee encryption of e-mail without company permission.
- Establish requirements for employee personal Web sites (indicate that the
  company name should not be posted on the site).
- Indicate the penalties for violations of the policy.
- Indicate that password protection does not guarantee freedom from employer
  access.
totally immune from liability for employee privacy claims. However, from the cases we have seen and others that have been decided, courts look favorably on employers who adopt an effective and well-implemented computer usage policy.

**GLOBAL ISSUES OF PRIVACY IN CYBERSPACE**

As an ever-increasing number of people access the Internet from all over the world, the question of what privacy should exist in cyberspace becomes all the more important. As national and international initiatives develop around the globe, significantly different perceptions of privacy begin to emerge, some in conflict with U.S. policy. The following section presents key initiatives around the world related to the issue of privacy in cyberspace.

**European Union Directive on Privacy Protection**

One of the most significant efforts protecting data privacy is the European Union’s (EU) Directive on Privacy Protection, which became effective on October 25, 1998. The directive 95/46/EC of the European Parliament and the Council of October 24, 1995, requires EU member states to adopt legislation that protects the “fundamental rights and freedoms” of an individual, particularly the right to privacy as it relates to the processing and collection of personal data. Under the directive, “personal data” is defined as “information that relates to an identified or identifiable natural person.” Corporations are not included under this definition. The definition of “processing” personal data is “any operation or set of operations performed upon personal data” and includes its collection, storage, disclosure, and destruction.

The provisions of the legislation also apply to nonmember states doing business with member states. Specifically, Article 6 of the directive requires member states involved in the collection and possession of personal data to ensure that the data are:

- Processed fairly and accurately.
- Collected for specified and legitimate purposes and not further processed in a way incompatible with those purposes.
- Adequate, relevant, and not excessive for the purposes for which they are collected and/or further processed.
- Accurate and, where necessary, updated.
- Kept in a form that permits identification of data subjects for no longer than is necessary.

---

The official name of the directive is the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
Additionally, Article 7 of the directive states that personal data may only be processed if the person or corporation in control of the data can prove at least one of the following:

- The consent of the data subject has been given unambiguously.
- The processing of the data is necessary for the performance or preparation of a contract to which the data subject is a party.
- The processing of the data is necessary in order to protect the vital interests of the data subject.
- The processing of the data is in the public interest or in the exercise of official authority of the controller of the data or a third party.
- The processing is necessary for the legitimate interests of the controller or a third party except where the data subject's privacy rights are greater.

One of the most important directives is Article 25. This article prohibits the export of personal data to nonmembers countries that do not have laws that “adequately” protect personal data. “Adequate” does not have a specific term, but is rather defined on a case-by-case basis “in light of all circumstances surrounding a data transfer operation or set of data transfer operations.”

Article 25 has significant implications for U.S. businesses and other EU nonmembers. This article requires EU members to follow vague minimum standards regarding the protection of personal data. For nations like the United States where its laws do not conform to the strictures of the directive, U.S. companies may be denied access to the EU marketplace. If U.S. companies “misuse” EU privacy information, they may be subjected to monetary penalties. Industries that heavily rely on personal data, such as services, travel, and health care companies, are most drastically affected.

Early implementation of the privacy directive has been quite stringent against EU nonmembers. For example, a Swedish privacy watchdog group demanded that American Airlines delete all health and medical information about Swedish passengers after each flight unless the passenger gave express consent otherwise. This would require American Airlines to delete details about allergies, asthma, and dietary needs, which are routinely collected in the United States, and not transmit that data to its SABRE reservation system in the United States. The Swedish court agreed with the privacy group, and transmission of this information was suspended.

This example also shows how easily anyone can take action against an infringing non-EU company. The directive permits any of the over 350 million EU citizens to file an action against a company claiming abuse of personal data that can be pursued to the highest echelons of the EU court system. At any time during this process, courts can mandate injunctions, suspend data flow, and halt business operations of an infringing firm. This first directive reveals how far apart the EU and other countries (especially the United States) are in their views of international data privacy.

**The United States/European Union Safe Harbor Agreement**

In response to the EU directive, the United States released draft “safe harbor” principles that purported to protect the privacy of data through a mix of government regu-
lation, registration, and industry self-policing. After significant negotiations, the EU and the United States reached an agreement on March 14, 2000, that established safe harbor privacy principles accessible to both parties. This agreement, known as The US–EU Safe Harbor Agreement, establishes fixed requirements that U.S. companies must satisfy in order to meet the EU's minimum standards of privacy protection. Meeting this standard would allow U.S. companies to avoid experiencing interruptions in their business dealings with the EU or avoid prosecution by European authorities under European privacy laws. Certifying to the safe harbor assures the EU that U.S. companies provides “adequate” privacy protection, as defined by the EU Directive. At least 130 companies have joined the list, with more additions on the horizon.

The safe harbor standard is focused on seven basic principles. The Seven Principles of the Safe Harbor Agreement, as stated by the U.S. Department of Commerce, are as follows:

1. **Notice:** Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers for limiting its use and disclosure.

2. **Choice:** Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, an affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.

3. **Onward Transfer (Transfers to Third Parties):** To disclose information to a third party, organizations must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent (1), it may do so if it makes sure the third party subscribes to the safe harbor principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such a third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.

4. **Access:** Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual’s privacy in the case in question or where the rights of persons other than the individual would be violated.
5. **Security**: Organizations must take reasonable precautions to protect personal information from loss, misuse, and unauthorized access, disclosure, alteration, and destruction.

6. **Data integrity**: Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

7. **Enforcement**: In order to ensure compliance with the safe harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so each individual’s complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self-certification letters will no longer appear in the list of participants and safe harbor benefits will no longer be assured.

If an organization fails to comply with the safe harbor after certifying it has done so, it will be actionable under federal and state law provisions prohibiting unfair or deceptive acts. If the failure to comply continues, the company will no longer be entitled to benefit from the safe harbor coverage, and the company must notify the U.S. Department of Commerce.

**Other National Efforts at Regulating Internet Data Privacy**

Nations outside the U.S. and EU spheres have also developed data privacy initiatives. The following efforts are examples of attempts to regulate data privacy around the globe.

**Australia.** Australia has recently enacted the *Privacy Amendment (Private Sector) Act 2000*, which establishes a national program for managing personal information by private firms. The act also allows industries in place of the legislative framework to develop privacy codes of their own that are tailored to their own industry needs. The legislation has been in force since December 21, 2001, although small businesses have an additional year to comply.

This legislation establishes ten *National Privacy Principles (NPP)* that are the minimum standards for the privacy sector. They regulate the collection, use and disclosure, and overseas transfer of personal data. The NPPs require that personal information is accurate, up to date, and secure. NPPs require that companies must disclose how they manage personal information, provide access and correction rights, and must allow individuals to deal with them anonymously if possible.

---

*The ten principles are collection, use and disclosure, data quality, data security, openness, access and correction, identifiers, anonymity, transborder data flows, and sensitive information.*
Chapter 9 Privacy

The act limits transmittal of information across borders. An organization can transfer personal information to someone in a foreign country only if the foreign individual is subject to a law or scheme that upholds principles of fair data handling that are substantially similar to Australia’s NPPs. Alternatively, the data may also be transferred if the individual who the information describes consents or it is necessary to perform or complete a contract. An individual who suffers harm from a violation of the act may collect damages from the controller or collector of the data.

Canada. Canada’s most recent endeavor in the privacy arena is the enactment of the Personal Information Protection and Electronic Documents Act, which became effective January 1, 2001. The act establishes basic ground rules regarding how private sector companies may collect, use, or disclose personal information collected by them in the course of their commercial activities.

With certain exceptions, the act requires a company to obtain an individual’s consent when it collects, uses, or discloses personal information. The act also requires companies to supply a consumer with a product or a service even if the consumer refuses to consent to the collection, use, or disclosure of personal information, unless the information is essential to the transaction. Companies must provide personal information policies that are clear, understandable, and readily available. Any information held by a company that remains after a transaction is completed with a consumer should be destroyed, erased, or made anonymous when that data is no longer necessary. The act does not apply to information held by individuals for personal use (e.g., a personal greeting card list), provincial or territorial governments, an employee’s basic personal information, and the collection of information solely for journalistic, artistic, or literary purposes.

If a complaint is filed, the privacy commissioner will investigate the complaint and attempt to resolve the dispute through mediation. That failing, the individual can ask for a hearing in the federal court. That court may award damages when appropriate. The court may also impose a fine as high as $62,790 ($100,000 Canadian) against any entity who inhibits a commissioner’s investigation.

Since passage of the act in 2000, Canada and the European Union have been working toward an agreement confirming an equivalent level of privacy protection in both jurisdictions. Part of the process examined whether the legislation was “adequate” under the EU Directive on Data Protection. In January 2001, the Article 29 Working Party (Data Protection), composed of privacy commissioners from all EU member states, considered the Canadian legislation and issued a favorable opinion on the level of privacy protection in Canada.

Russia. The Russian Federation has taken a diametrically opposed view to data privacy. In short, the Russian government has given itself the power to spy on its citizens when they use the Internet. Further, Russia can punish Internet service providers (ISPs) that will not help. In 1999, Russia’s Federal Security Bureau (FSB), formerly known as the KGB, introduced an addendum to a regulation called System for Operational-Investigative Activities (SORM). The addendum requires an Internet service
provider to install government-supplied "black boxes" that monitor electronic communications. ISPs are required to pay for the new technology. ISPs that refuse may be shut down. Security agencies may be tempted to bypass the legal requirement for a warrant before monitoring private correspondence. In early 2000, that power was expanded beyond the FSB to seven other federal security agencies, including the tax and interior ministry police.

Summary

This chapter discussed the common law and constitutional sources of the right to privacy, applying them to cyberspace. It also discussed the many federal statutes that have been passed to protect this right, including those related to personal identifiable information contained in financial and health care related records and data. Major emphasis was placed on the Electronic Communications Privacy Act. Employer-employee workplace privacy issues and policies were also explored. Spamming and its conflicts with First Amendment rights were also highlighted.

Finally, in the international arena the EU data privacy directive has set the standard for global data management. U.S. companies may now satisfy the directive requirements by applying under the US–EU Safe Harbor Agreement reached in 2000.

Key Terms

Fourth, Fifth, and Ninth Amendments to the U.S. Constitution, 258–259
Intrusion upon Seclusion, 260
Public Disclosure of Private Facts Causing Injury to Reputation, 260
Publicly Placing Another in a False Light, 261
Misappropriation of a Person’s Name or Likeness Causing Injury to Reputation, 261
USA Patriot Act, 268
Privacy Protection Act (PPA), 268
Privacy Act, 268
Cable Communications Protection Act (CCPA), 269
Video Privacy Protection Act (VPPA), 270
Telephone Consumer Protection Act (TCPA), 270
Fair Credit Reporting Act (FCRA), 270
Computer Fraud and Abuse Act, 271
Bank Secrecy Act, 271
Right to Financial Privacy Act, 272
Gramm-Leach-Bliley Act (GLB), 272
identity theft, 273
pretexting, 274
Health Insurance Portability and Accountability Act (HIPAA), 274
Children’s Online Privacy Protection Act (COPPA), 275
Electronic Communications Privacy Act (ECPA), 276
Business Extension Rule, 278
Carnivore, 280
spam, 284
fair information practices, 286
“spoofing,” 286
netiquette, 287
The US–EU Safe Harbor Agreement, 303
Seven Principles of the Safe Harbor Agreement, 303
Privacy Amendment (Private Sector) Act 2000, 304
Personal Information Protection and Electronic Documents Act, 305
System for Operational-Investigative Activities (SORM), 305
Manager's Checklist

✓ Make sure company use of the Internet and Web are mindful of rights to privacy.

✓ Establish and implement effective company privacy policies regarding e-mail and computer usage. Make sure you establish a level of privacy employees should “reasonably expect.”

✓ Take steps to protect privacy and confidentiality of company-related proprietary interests and data, especially related to personnel.

✓ Make sure you and your employees are aware there is very little privacy protection afforded to online communications.

✓ If your company collects and stores information about its customers, make sure you provide them with an easy-to-read privacy policy (follow the fair information practices) with an opt-in rather than opt-out provision.

✓ Be familiar with all applicable privacy laws and regulations, especially the fair information practices recommended by the FTC. Consider adopting the TRUSTe or other seal of approval for your Web site.

✓ Implement a policy of self-regulation regarding privacy rights, including the kind of netiquette that others have established.

✓ Ensure that any international data gathering effort complies with the EU directive on privacy. Satisfying the safe harbor provisions should be considered a perquisite for doing online business in Europe.

✓ Be aware that national approaches to data privacy vary widely. Russia, for instance, has little if any privacy protections for consumers and businesses.

✓ Ethical Considerations

Be truthful and forthright with employees regarding monitoring and computer usage policies and expectations. You and other company executives must adhere to them as well.

If your company collects and uses personal identifiable information about its customers and expresses a concern for their privacy, ensure that concern is reflected in actions and not merely words.

Support industry initiatives such as P3P, TRUSTe, and Netiquette.

Case Problems

1. Curtis and other plaintiffs, former at-will employees of Citibank, brought this action for sexual harassment under Title VII of the Civil Rights Act of 1965.
against DiMaio and other defendants alleging the defendants created a hostile work environment when they used Citibank’s e-mail system to send them e-mails that contained two racially and ethnically jokes offensive to African Americans. The defendants admitted the jokes were insensitive but that sending only two jokes was not severe or pervasive enough to have created a hostile workplace and satisfy the requirements of Title VII. How should the court decide? Give reasons for your answer. [Curtis v. DiMaio, 46 F. Supp. 2d 206 (E.D. N.Y. 1999), affirmed, 205 F.3d 1322 (2d Cir. 2000)].

2. Plaintiff, Steve Jackson Games (SJG), publishes books, magazines, role-playing games, and related products. In the mid-1980s, it began operating a BBS that offered its customers services by which could be sent and received. Private e-mail could be stored on the hard drive of its BBS until retrieved by the addressee. An investigator for the Bell Company discovered SJG was distributing a computerized text file containing information about Bell’s emergency 911 call system. The Secret Service was notified and obtained a warrant and seized SJG’s computer that operated the BBS, thereby closing it down. No 911 document belonging to Bell was found. When it was returned sometime later, SJG discovered 162 e-mail messages had been read and deleted. SJG sued the Secret Service, claiming violations of the Privacy Protection Act and Title I and II of the ECPA. The lower court found a violation of Title II because the Secret Service unlawfully seized stored electronic documents. However, because the Secret Service did not “intercept” the e-mail wrongfully (it had not acquired its contents contemporaneously with its transmission), it held there was no violation of Title II. Do you agree with the court’s findings? [Steve Jackson Games v. U.S. Secret Service, 816 F. Supp. 432 (W.D.Tex. 1993), aff’d 36 E. 3d 457 (5th cir. 1994)].

3. The plaintiff, a senior executive-level employee, is allowed to use the defendant’s company-owned computer for work at home. He agreed to and acknowledged the defendant’s computer usage and monitoring policy. The defendant monitors and inspects the computer, discovering the plaintiff had been accessing pornographic Web sites. The plaintiff claims the Web sites had simply “popped up” on his computer screen. He is fired and sues for wrongful termination alleging that because the computer was provided as a perk for senior executives so they could work at home, he enjoyed a reasonable expectation of privacy. The defendant disagreed, claiming his actions were legal. What result? [Zieminski v. TBG Insurance Services, Inc., No. B153400 (Cal. Super. Ct., 2002)].

4. GeoCities operates a very popular Web site with more than 2 million members (200,000 are between the ages of 3 and 15), which it refers to as “Home­steaders.” Geo provides numerous services to its members, including free and fee-based home pages and free e-mail service. To join, individuals must com-
plete a new member application form in which mandatory personal information is required. The application also requests other “optional” information about level of education, income, marital status, and occupation. In the form, members were told their information would only be used to “provide members the specific advertising offers and products and services they requested and that the ‘optional’ information would not be released to anyone without the member’s permission.” The Federal Trade Commission (FTC) issues a complaint against Geo, alleging it engaged in deceptive practices by selling or disclosing personal information about its members, including children, to third parties other than those agreed to. These third parties would then be able to send unsolicited advertisements to these members. Geo denies the allegations.

What should GeoCities do in order to avoid claims that its actions are violating the privacy rights of its members including those between the ages of 3 and 13?

5. Plaintiffs are consumers who visit the Web sites of the defendants who are drug companies. These companies hired co-defendant, Pharmatrak, a provider of Internet traffic tracking services, to place cookies on plaintiffs’ hard drives in order to secretly intercept and access the plaintiffs’ electronic communications and visits to the defendant’s Web sites. This was done without plaintiffs’ knowledge, authorization, or consent. Personal information was collected about the plaintiffs related to their browsing habits and health. Pharmatrak provided monthly traffic reports to the drug companies. There was no evidence the information collected was being used unlawfully. The plaintiffs claim the actions of the defendants violated their privacy rights under Title I and II of the ECPA. The defendants claim they qualify for the “consent” exception provided under § 2511 (2)(d) of the ECPA. Are they correct? Do the plaintiffs have any privacy rights under HIPAA? [In Re Pharmatrak Privacy Litigation, 2002 WL 1880387 (D. Mass)]

6. In May 1999, officials from the Spanish Data Protection Authority carried out an inspection of Microsoft’s subsidiary in Spain. The authority found that Microsoft possessed a database filled with the personal information of their Spanish consumers. It was later determined that Microsoft was transferring Spanish employee information from Spain to a Web server in the United States. Under current international law, what was the result?

Additional Readings


• Verton, Dan. “Government Data Mining Raises Privacy Concerns.” *Computerworld* (January 17, 2003) ([http://www.computerworld.com](http://www.computerworld.com)).