

NETLAW

"A must read for anyone needing to know their rights and obligations when they go online."

Wayne Greenberg,
President and G.M.,
Shepard's

Your Rights in
the Online
World

*The Guidebook to the
Changing Legal Frontier*

Lance
Rose



WILEY

WILEY

NetLaw:

Your Rights

in the Online World

Lance Rose

Osborne McGraw-Hill

Berkeley New York St. Louis San Francisco
Auckland Bogotá Hamburg London Madrid
Mexico City Milan Montreal New Delhi Panama City
Paris São Paulo Singapore Sydney
Tokyo Toronto

Osborne **McGraw-Hill**
2600 Tenth Street
Berkeley, California 94710
U.S.A.

For information on software, translations, or book distributors outside of the U.S.A., please write to Osborne **McGraw-Hill** at the above address.

NetLaw: Your Rights in the Online World

Copyright © 1995 by Lance Rose. All rights reserved. Printed in the United States of America. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

34567890 DOC 99876

ISBN 0-07-882077-4

Publisher:
Lawrence Levitsky

Acquisitions Editor
Scott Rogers

Project Editor
Claire Splan

Copy Editor
Gary Morris

Proofreader
Pat Mannion

Indexer
Valerie Robbins

Computer Designer
Peter F. Hancik

Illustrator
Helena Charm

Series Designer
Lance Ravella

Cover Designer
Mason Fong
Background painting: Charlie Owen

Quality Control Specialist
Joe Scuderi

Information has been obtained by Osborne **McGraw-Hill** from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, Osborne **McGraw-Hill**, or others, Osborne McGraw-Hill does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from use of such information.

This publication is designed to provide authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional service. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

About the Author

Lance Rose, Esq. is nationally recognized in the field of online law. He writes regularly for *WIRED Magazine* and *Boardwatch Magazine*, and is a moderator on LEXIS Counsel Connect, an online system for attorneys. He also speaks at and helps organize various national conferences, seminars, and trade shows. Mr. Rose was co-author of *Syslaw*, published in 1992.

As an attorney, Mr. Rose has been involved in computer law since 1982, and online legal matters since 1986. His firm, Lance Rose & Associates, in Montclair, New Jersey, works with many kinds of businesses in the online world including electronic and print publishers, online services, electronic payment businesses, Internet providers, system operators, content providers, and software developers and publishers. He has a J.D. cum laude from Benjamin Cardozo School of Law, and an LL.M. in Intellectual Property/Trade Regulation from New York University School of Law.

Acknowledgments

There are many whose influence must be acknowledged. I'm sure I'll miss a few, so please accept my humblest apologies in advance.

- My wife Janet and daughter Julietta, who with divine patience humored me while I stole from my time with them to work on this book.
- My once-partner Jonathan Wallace, co-author of *Syslaw* way, way back in 1989. That's prescience! His sense of fairness and balance hopefully live on in the newly incarnated *NetLaw*.
- My associate and co-worker Steve Barber, Esq., who helped with the book at critical points and saved me from certain death by deadline.
- The editors and other folks at Osborne/McGraw-Hill, especially Scott Rogers, who can keep authors happy while retaining his dignity; his assistant Kelly Vogel; project editor Claire Splan; and Editor-in-Chief Jeff Pepper.
- Those who added meaningfully to my understanding of online law, business, or culture, including Joe Abernathy, John Perry Barlow, Ann Branscomb, Bill Frezza, Mike Godwin, Stacy Horn, David R. Johnson, Charles Merrill, Jerry Michalski, Henry Perritt, Jack Rickard, Neil Shapiro, Mark Stahlman, Brad Templeton, Jim Warren, Don Watkins, Larry Wood, and Ben Wright.
- Plus the hundreds of others I've chatted with or whose articles or books I've read the past few years in connection with the growth of online society, all of whose insights can undoubtedly be found mingling among the observations in these pages.

Needless to say, the errors in this book are all of my own fiendish invention, and should not be blamed on any of the gentle souls named above.

Introduction

What is Online Law?

Millions of individuals are exploring computer networks and online systems today. Did I say individuals? Look again. Everywhere on the Net, *groups* of people gather—on bulletin boards, in Usenet, in chat rooms, and other places online. They're socializing, doing business, publishing to each other on the World Wide Web. It is more than just having fun with computers and modems. It is the start of a social revolution, perhaps the most important structural advance in society in our lifetime.

The new social revolution is not about technology at all, though we needed technology to make it happen. Its essence is deceptively simple: people coming together from all points of the globe to meet on the common ground of the Net. We never had this ability before, in the entire history of civilization. We created the Net when we connected computers to telephone systems, and put those computers in a lot of homes and offices.

In the past, social groups did not function unless their members were close together. If you threw a party, your guests came in from a few miles away. Corporations kept their brass concentrated near the headquarters office. The strength of civic groups depended on how often they could get their members together in the same room. There have always been more extended parties, corporations and associations, of course, but until now they could conquer physical distance only through brute force: spending lots of time and money carting people from where they lived to where they could meet with others. It was a game only the very rich or extremely dedicated could afford to play. The rise of the voice telephone system changed things a little, but it remained almost entirely a one-on-one medium. Networks and online services, in contrast, readily support online communities of almost any size.

Now we can gather together online with ease. It is getting easier and cheaper every day. People are starting to live parts of their lives online, in discussion groups, clubs, trade organizations, virtual corporations, and so on. We can help each other and enrich each others' lives in ways previously unimagined. We are bursting out of the shared blinders worn by geographically provincial groups, to achieve new, globally informed perspectives and ways of working together.

At the same time, new opportunities for misunderstanding arise, often with people we may never meet in the flesh. The Net is revolutionary in supporting social and business groups spread across countries and continents, but it does not portend any immediate change in individual human nature. Just like in the physical world, people and businesses can hurt others on the Net in a lot of ways, both accidentally and on purpose. They can tell hurtful lies about each other, steal or wrongfully

copy each others' property, reveal painful or damaging secrets, or break a promise or a deal on which someone else depends. This is not merely theoretical. There has already been plenty of real damage caused to others through the Net.

For approximately the first three decades of the Net's existence, from the '60s through the '80s, little of the damage caused online led to legal action of any kind, apart from government agents busting a few "phone phreaks" for long distance pranks, or software companies shutting down pirate bulletin boards bulging with infringing "warez." The first Net users were explorers charting the wilderness, not litigious businessmen. Besides, most injuries on the Net could not be measured in money. Since our land-based courts require significant sums as the price of admission, they were simply not involved in early Net conflicts. With courtroom resolution out of the question, those injured online had few alternatives. They could try to injure the person who injured them; they could appeal to those controlling Net resources to cut off the wrongdoer; or they could simply retire from the Net and get back to the physical world, where all the real action was at the time anyway.

Things have changed. Now there's lots of money, people, and businesses on the Net. Many billions of dollars are being invested today in its further development as a social and business environment. This in turn has opened the doors to the land-based courts, who are now becoming deeply involved in online law for at least three reasons. First, there are now a lot of rich folks and companies on the Net, who can easily afford to sue those who hurt them online. Second, the companies investing billions in Net development want to protect their hefty investment. They will readily shave off millions of dollars and fund as many lawsuits as necessary to secure their online assets and business opportunities. Third, all the attention that our society is now giving to the Net, including all the hype about the "National Information Infrastructure," the "Information Superhighway," and "telecommuting," inevitably rubs off on the courts and legal systems. Judges are more likely to recognize the Net as a place where people meet and do business, where wrongful acts can lead to real injuries deserving of a legal remedy. Again, this is not merely an academic point. We are seeing a sharp, steady rise in lawsuits based on events that took place largely or wholly on the Net.

Which leads to the question: which legal system applies to the Net? The answer may change over time, but for now, U.S. citizens should assume they can be called to appear in state and federal courts in the U.S. if they injure others on the Net. The land-based governments and courts have power over our bodies. If someone injured on the Net asks a court to decide a dispute with a U.S. citizen, the court will call that citizen in to defend the lawsuit, using marshalls and guns if necessary to back up its demand.

Once in court, another question arises: what rules or laws should apply to disputes arising on the Net? Once again, U.S. citizens should assume that in legal matters involving other U.S. citizens, state and federal laws of the U.S. will be applied. Courts today are not close to recognizing special legal jurisdictions on the Net, and it may be years or decades before they do. The reality today is that U.S. laws are applied routinely to events online, as demonstrated in several of the cases listed in Appendix K.

There is currently a partial way out of the straight application of U.S. laws to Net activities. It was pioneered many years ago by banks using online funds clearing systems, and investors using online trading systems like NASDAQ: membership agreements, where participants in an online group agree to rules that will govern their mutual affairs. U.S. courts readily treat such agreements as legal contracts, setting up self-contained legal systems with their own rules and logic. Thus, any group of people running or involved in an online system can take hold of much of their own legal destiny, simply by agreeing to set their own rules by mutual agreement.

These group agreements are limited, however, whenever they conflict with overriding state or federal public policies. Such policy limits are often not hard to divine. For instance, let's say an online

membership group sets up a massive bartering market where goods are traded directly for other goods with no money changing hands, and the IRS brings group members to federal court to make them report and pay taxes on the transactions. We can expect that the courts would readily apply U.S. tax law to their activities, brushing aside any suggestion that the group's internal agreement that no money changes hands makes the Internal Revenue Code inapplicable.

It is within this existing regime—that U.S. courts and U.S. laws will regularly be applied to people and businesses who can be found in the U.S.—that *NetLaw* is set. In the chapters to follow, we will explore the subjects of greatest legal importance on the Net today. Much of what we will demonstrate is how traditional legal thinking needs to take into account the many new social and business environments found on the Net. The reference point is always U.S. law, though the techniques applying that law to the Net may be instructive to those in other countries who are working out how their own laws will apply to the Net.

At the same time, we will hopefully show how the Net is not automatically a "whole new ball game." The Net is not populated by a new set of people. Everyone using the Net is deeply entrenched in the land-based world, and sharing the heritage of thousands of years of land-based cultural and social development. We bring that history with us when we go online. Whether we view our heritage as an asset or as wasteful baggage, groups of people instinctively erect their acculturated understandings all around them in the Net. As a result, legal scenarios online will look very, very familiar to those of us who have spent any time in the physical world.

Working with and within online law is a learning process in its very earliest stages. It is not, however, nearly as mysterious as some newcomers to the field suggest. Even without a lot of court decisions or legislation specific to the online world to guide us, we can say a lot about online law today based on what we know about existing laws and their evolution, the social goals and pressures at play on the evolving Net, and common sense. It is the goal of *NetLaw* to arm the reader with enough information in all these areas to proceed with confidence into any social or business situation on the Net. In the meantime, unanswered legal questions will remain online, just as they do in the physical world. They are a permanent condition in an evolving society.

What Is in This Book

The book has eight chapters, each covering an important legal area in the online world.

1. "Freedom, Censorship, and Control of the Online System"—Who controls online systems, and what are the limits of that control? Is it legal to censor Net users? The First Amendment guarantees "freedom of speech." We will look at how freedom of speech works online, and see how it is the most important law in the U.S. protecting the Net, its users and its providers today.
2. "Contracts and Commercial Arrangements"—How do you use contracts to manage your risks online, and set up the kinds of online relationships you want. What are the terms of basic user agreements with online services and access providers? For those who do business on the Net, what deals should they make with customers and suppliers?
3. "Owning and Using Online Property"—In the past, most information was freely transmitted on the Net. Today, information freedom is under pressure from copyright owners setting up their shops online. What are the rules covering our use of messages and files belonging to others? How do the copyright and trademark laws work online?

4. "Dangers and Responsibilities in the Online World"—There are many kinds of injury on the Net, such as libel, infringing copyrights, and trafficking in stolen credit card numbers. What legal standards of conduct apply online? What is the risk to corporate managers when their in-house LANs are connected to the Net? Should system operators be blamed for injuries caused by those who use their systems? There is a great deal of concern today over network security. What legal obligations are there to keep an online system secure from intruders?
5. "Privacy"—Our privacy is increasingly threatened, and seems to become more precious as we live more of our lives on the computer networks. Does the law protect our privacy on the Net? Can businesses rely on legal protection for their trade secrets? Encryption software is becoming increasingly popular as a way to keep e-mail entirely secret. Are there legal limits to its use?
6. "Crime and the Online System"—What counts as a crime when you're online? We look at how federal and state computer crime laws apply in the online world. We also look at what you can do when you see someone committing a crime online, and when a system operator might be held responsible for criminal acts committed on the system.
7. "Searches and Seizures"—Government agents have been known to stage raids on online systems, and carry the computer equipment away for inspection. They have also been known to make mistakes, as in the famous case of Steve Jackson Games. What laws protect online systems and materials from search and seizure, and how can system operators minimize their risks?
8. "Adult Materials and Themes"—Adult materials and services are among the most active uses of the Net today. They are also often among the most illegal; adult online services advertising nationally one month can be under criminal indictment the next. We will look at the laws regulating obscenity, child pornography and indecent speech, and the Constitutional limits against state and federal prosecution.

In addition, extensive appendixes provide a variety of resources, including sample contracts, case citations, statutory texts, and pointers to other sources of information.

How to Use This Book

This book is meant to help readers know which behavior is legal, and which illegal, when they encounter it on the Net. Most Net users and operators need such a primer today. In the physical world, we know inherently about many things that are illegal, even if we never opened a law book or talked to a lawyer: shoplifting; robbing banks; driving the wrong way down a one way street; killing or injuring people; counterfeiting money or forging checks; selling dangerous products, from cars to breast implants; breaching a contract. How do we know these things? They are presented to us continuously in the media, in school, and by our parents and friends. They are the kinds of harmful activity our society knows it will not tolerate. Those who ignore the basic teaching, who carelessly cross the clear lines of illegality, could find themselves in court defending a suit for money damages or a criminal indictment.

In contrast, most people have no such background in online law, no history of examples where people did the illegal or harmful act, then got hauled into court. We cannot rely on a common knowledge of online law threading through society and culture, because it is simply not there yet.

Even when we assume that laws born in the physical world apply online, there remains the question of *how* do they apply?

That is where this book comes in. *NetLaw* can serve as a guide to the major laws and legal events today in the online world. It is also like a first aid manual: it helps the reader identify legal risks and rights for online systems, explains the causes behind them, and suggests ways in which the reader can protect their rights, and handle or avoid the risks.

For instance, if you wonder whether your privacy rights were violated on a given online system, or if you simply want to know more about the general framework of privacy rights on computer networks, you can go right to the privacy section of this book and read up. You don't have to plow through unrelated materials on computer crime or online dealmaking to figure out the score on privacy. Or you may be concerned about your company's legal responsibility to keep the in-house system secure from intrusive hackers. To learn more about it, you can look at the sections on security and related subjects in Chapter 4.

When used in this way, the book is a practical reference to be picked up and consulted whenever you encounter new legal issues on the Net. Where it does not provide an answer, the resources listed in the appendixes will show you where you can investigate further.

If you prefer, you can read the book cover to cover for a tour of the online world as it exists today and the legal tangles to which it has been host. Reading about legal matters online is one way of tuning into the drama of the Net. It is also a way to develop an understanding how the law meshes with other aspects of online culture and society.

Scattered throughout the book are two kinds of text boxes. One kind, indicated by a picture of the scales of justice, features discussions of various trends affecting the development of online law. Very few cases involving online law—less than a handful—have been decided in the two or three years since the last revision of this book (previously published under the title *SysLaw*). However, in that same time there has been a whirlwind of activity very important to how online law will develop in the next few years: new and attempted legislation; disagreements between companies, organizations, and industry groups, which may lead to lawsuits; social and business developments with obvious legal consequences down the line. These events are only potentially significant, their precise impact too vague for them to be presented as part of online law as it exists today. However, we must still track these nascent trends to understand online law as it evolves. By placing this material in boxes, we've separated it from what might be considered the better established "law" that applies online, yet highlighted its importance to understanding how online law may evolve over time.

The other kind of text box presents to the reader various metaphors that Net users apply to different parts of the online world. Each such box is graced with a picture of one of these metaphors. The special focus on metaphors reflects the peculiar path by which legal analysis and lawyers tend to approach legal affairs on the Net: by analogizing online matters to supposedly similar past events in the physical world. This phenomenon is not limited to the legal profession by any means. How many times have we all heard references to online systems being like printing presses, telephone systems, postal systems, book stores, libraries, inns, or highways?

Whether we admit it or not, metaphors underlie some of our most strongly held convictions about the Net. It is now time to get more serious about these models, to understand where it is valid to compare them to Net phenomena and where the comparisons must end. The goal of the metaphor boxes in this book is to begin the job of inspecting the metaphors and see what light they shed in understanding online law. Even the little pictures are part of this effort. They provide a visual cue for the reader, an additional path to the reader's own rich store of mental associations which flesh out the full meaning of each metaphor as it is applied to the virtual world online.

The text boxes provide, then, yet another way of reading this book. The reader can skip from box to box as if reading a magazine, and build a collage-like sense of how law is developing online and the metaphorical world in which it operates. There is some overlap of material between the text boxes and the main text. This is deliberate. Many of the events taking place online have multiple meanings and implications for online law and society, and are best portrayed in multiple contexts. In this book, we accomplish this by referring to certain key events at different points in the discussion, and within different types of discussions.

Terminology relating to the online world is used rather loosely here, mirroring the degree to which it is still unsettled among those who use online systems. You will see "online world" used a lot here, because it's simple, attractive, and accurately portrays the sense that those who communicate online regularly feel as though they operate in a shared world. The term "cyberspace" looks at this time like it might become the word of general usage for referring to this same realm, so it is also used interchangeably with "online world" in this book. "Internet" refers to the TCP/IP network of networks that evolved out of the ARPAnet of the '60s. The term "Net," on the other hand, refers to the online world as a whole, and emphasizes the connectedness of all online points to all other points (though for any two physically unconnected networks, the connection is via the people who participate in both). If this is a bit confusing, don't worry. All these terms refer generally to the big online arena within which people are socializing and conducting businesses, and within which deals can be made and laws can be broken. Other terminology is fairly straightforward: "user" means a person using an online system; "operator" means someone running an online system or service of any kind; and "online system" means any kind of online service or operation, including BBSs, newsgroup conferencing systems, mailing lists, echo conferences, and MUDs.

Remember, the information in this book is information only, and *not legal advice*. It is for readers to add to their own knowledge of how law works in the online world, so they can perform their own legal analyses armed with more and better information. For definitive help on any given legal situation, the reader should track down a lawyer competent in the practice of online law. If one can't be found, then find a good lawyer with an open mind, and show him or her a copy of this book so they too can jump into the practice of online law.

Contents

| | | |
|----------|--|-----------|
| 1 | <i>Freedom, Censorship, and Control of the Online System</i> | 1 |
| | Freedom of Speech and of the Press | 1 |
| | The First Amendment | 2 |
| | Media and Free Speech—Inconstant Companions | 3 |
| | The Social Power of the Computer Bulletin Board | 4 |
| | We Are All Broadcasters | 5 |
| | How Does the First Amendment Protect Online Systems and Users? | 6 |
| | The Publisher/Distributor Distinction | 8 |
| | Taxing Channel One | 8 |
| | The Online System as Print Publisher | 10 |
| | System Guilty, Operator Innocent? | 12 |
| | The Online System as Telephone Service | 14 |
| | The Online System as Magazine Distributor | 16 |
| | The Online System as Bookstore | 18 |
| | Music Publishers Rally Against CompuServe | 20 |
| | Computer Networks as Public Streets | 23 |
| | Growing Pains Online and Off | 26 |
| | The Online System as Local Bar | 27 |
| | Speaking of Education | 29 |
| | Structuring the Online System | 30 |
| | Controlling User Speech: System Management, or "Censorship"? | 31 |
| | Whether to Join a Network | 34 |
| | Whether to Run an Online System for Profit | 35 |
| | The Freedom to Continue or Quit | 36 |
| | | |
| 2 | <i>Contracts and Commercial Arrangements</i> | 39 |
| | What Is a Contract? | 40 |
| | What Matters Do You Cover in a User Contract? | 40 |
| | "Hey Internet Kid, Wanna Green Card?" | 41 |

| | |
|---|----|
| Access and Services Provided to Users | 42 |
| Price and Payment | 44 |
| Digital Cash: Long Green Online | 45 |
| Limitation of Liability | 46 |
| Indemnities | 47 |
| Privacy | 48 |
| Editorial Control | 49 |
| Ownership of Messages | 50 |
| Contracts and Corporate Systems | 51 |
| In-House Systems | 52 |
| Customer Support Systems | 54 |
| Commercial Arrangements Between Online Businesses | 55 |
| General Concerns | 55 |
| Taking the Internet Private | 56 |
| The Online System as a Shopping Mall | 58 |
| Virtual Corporations | 60 |
| Data Provider Agreements | 64 |
| The Online System as a Toll Road | 66 |
| Basic Communications Utilities | 70 |
| Gateway Arrangements | 71 |
| Online Space Rentals | 72 |
| Other Agreements | 77 |
| How Do You Form a Contract? | 78 |
| Online User Contracts | 78 |
| Other Online Contracts | 79 |
| More Reliable Than Pen and Ink | 80 |
| Written Agreements with Users | 81 |

3 *Owning and Using Online Property* 83

| | |
|---|-----|
| Brief Introduction to Copyright Law | 84 |
| Copyrights Online—Nothing New, or Vast Expansion of Rights? | 85 |
| Is Copyright Dead? | 87 |
| A Special Infringement Rule for Online Systems? | 91 |
| The Public Domain | 92 |
| Copying Within the Law | 94 |
| Giving Information Back to the Taxpayers | 94 |
| Public Messages from Users | 97 |
| E-mail | 99 |
| Files | 99 |
| Computer Program Files | 99 |
| Shareware, Freeware, and Public Domain Software | 100 |
| Text Files | 102 |
| Image Files | 102 |
| Writers Fight for Their Electronic Rights | 103 |

| | |
|--|-----|
| A Picture Within a Picture | 105 |
| Sound Files and MIDI Files | 106 |
| Music Files on Networks: Publishing or Broadcasting? | 107 |
| Databases | 109 |
| Structure of the Online System | 111 |
| CD-ROM Jukebox Online! | 112 |
| Confidential Business Information as Property | 114 |
| Trademarks | 114 |
| The Name-Blocking Game | 116 |

4 ***Dangers and Responsibilities in the Online World*** **119**

| | |
|---|-----|
| The Online World as the Wild West Frontier | 120 |
| Degrees of Wrongful Conduct | 122 |
| Deliberately Wrongful Acts | 122 |
| Reckless Conduct | 122 |
| Negligent Conduct | 123 |
| The Online System as Supermarket | 124 |
| Killers for Hire—Would You Take Their Ads? | 127 |
| Particular Dangers and Risks | 128 |
| Defamation | 128 |
| Are the Courts Necessary to Combat Online Defamation? | 130 |
| Right of Privacy | 131 |
| Erroneous Information | 133 |
| Copyright Infringement | 134 |
| Access or Security-Related Information | 135 |
| The Long Arm of the Law | 136 |
| Maintaining System Security | 138 |
| The Major Security Threats: Viruses and Intruders | 138 |
| The Duty to Maintain a Secure System | 143 |
| The Responsibility of Managers and Other Employees | 149 |
| Company Responsibility for Its Agents and Employees | 151 |
| Managing Risks | 153 |
| Avoiding Self-Created Problems | 153 |
| Contracts | 153 |
| Security Measures | 154 |
| Warnings and Bulletins | 155 |
| There's a Sucker Logging on Every Minute | 156 |
| Incorporating | 157 |
| Insurance | 159 |
| Deal Effectively with All Known Risk Situations | 159 |
| Monitoring User Activity | 160 |
| Blame the User, Not the Messenger | 161 |
| "You Own Your Own Words" | 163 |

| | | |
|----------|---|------------|
| 5 | <i>Privacy</i> | 165 |
| | Nothing to Fear but the System Operator Himself | 166 |
| | Electronic Communications Privacy Act ("ECPA") | 167 |
| | Voice Messages | 168 |
| | Non-Voice Messages | 168 |
| | The Online System as a Postal Service | 169 |
| | The ECPA and Government Authorities | 170 |
| | The Information SnooperHighway | 170 |
| | Violating the ECPA | 171 |
| | Negotiating Privacy Under the ECPA | 172 |
| | Piggybacking on User Privacy | 173 |
| | Other Privacy Laws | 175 |
| | The Online Service as Private Home | 176 |
| | The Market Defeat of Lotus Marketplace | 178 |
| | Privacy in the Workplace | 179 |
| | Self-Help Privacy: Encryption | 181 |
| | Pleased to Meet You, You Can't Guess My Name | 183 |
| | Strategies Regarding User Privacy | 185 |

| | | |
|----------|---|------------|
| 6 | <i>Crime and the Online System</i> | 187 |
| | Confusion or Convictions? | 189 |
| | Crimes Against the Online System and the Operator | 190 |
| | The Computer Fraud and Abuse Act ("CFAA") | 190 |
| | Hackers and the Law | 192 |
| | Electronic Communications Privacy Act ("ECPA") | 193 |
| | New York State Computer Crime Statute | 194 |
| | Next Time, Use a Collection Agency | 197 |
| | What to Do About Criminal Activity Against a System | 198 |
| | Use of the Online System to Commit Crimes | 200 |
| | Kinds of Crimes That Can Be Committed on Online Systems | 201 |
| | The Evil Some System Operators Do | 201 |
| | Ways That System Operators Might Be Criminally Liable | 202 |
| | The Online System as Casino | 204 |
| | Online System Seizure Where the System Operator Is Not a Suspect | 207 |

| | | |
|----------|---|------------|
| 7 | <i>Searches and Seizures</i> | 209 |
| | What Are the Rules? | 210 |
| | LambdaMOO, Mr. Bungle, and the Rebirth of Due Process | 210 |
| | Caution—FBI at Work | 214 |

| | |
|--|-----|
| Special Restrictions Against Police Activity Under the ECPA | 215 |
| Special Restrictions Against Police Activity Under the Privacy Protection Act | 217 |
| The ECPA and PPA Compared | 219 |
| When the Police Knock on the Door | 220 |
| The Show Biz Cops of Oklahoma City | 222 |
| After the Search or Seizure | 223 |
| What Really Happens? | 225 |
| Steve Jackson Games | 225 |
| We Took Your Computers, But Forgot the Charges | 225 |
| The Smaller They Are, the Harder They Fall | 229 |
| Other Seizures | 230 |
| Why Do These Problems Occur? | 231 |
| The Online System as a Dangerous Gadget | 233 |
| Avoiding Trouble Before It Starts | 234 |
| Know Your Users | 235 |
| Bulletins and Other Public Statements | 235 |
| Act Immediately on All Suspicious Materials or Activities | 237 |
| Dealing with the Problem User | 237 |
| The Connecticut Bomb Factory | 238 |
| Civil (Non-Criminal) Seizures | 240 |
| Do You Get Advance Warning of the Civil Search or Seizure? | 241 |
| After a Civil Seizure | 242 |

8 *Adult Materials and Themes* 245

| | |
|---|-----|
| The Online System as Adult Bookstore | 246 |
| Sell Porn for Instant Online Success! | 247 |
| Which Laws Apply? | 248 |
| How Is "Obscenity" Defined? | 250 |
| Which Community's Standards Apply? | 250 |
| The Online System as Singles Bar | 252 |
| Obscene, or Merely Indecent? | 253 |
| Exon Amendment—Good or Bad? | 254 |
| Child Pornography | 256 |
| What Can Government Authorities Do to an Online System? | 257 |
| The Video Guy Down the Street Does It | 257 |
| How to Avoid or Reduce the Risks | 258 |

A *Sample Contracts* 261

| | |
|---|-----|
| Sample Contract 1: User Agreement for Online Services | 262 |
| Sample Contract 2: System Operator Agreement | 267 |

| | |
|--|-----|
| Sample Contract 3: Information Provider Agreement | 271 |
| Sample Contract 4: Online Space and Services Agreement | 276 |

B *Electronic Communications Privacy Act* **283**

| | |
|---|-----|
| Wire and Electronic Communications Interception and Interception of Oral Communications | 283 |
| § 2510. Definitions | 283 |
| § 2511. Interception and disclosure of wire, oral, or electronic communications prohibited | 286 |
| § 2512. Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited | 291 |
| § 2513. Confiscation of wire, oral, or electronic communication intercepting devices | 292 |
| § 2514. [Repealed] | 292 |
| § 2515. Prohibition of use as evidence of intercepted wire or oral communications | 292 |
| § 2516. Authorization for interception of wire, oral, or electronic communications | 292 |
| § 2517. Authorization for disclosure and use of intercepted wire, oral, or electronic communications | 295 |
| § 2518. Procedure for interception of wire, oral, or electronic communications | 295 |
| § 2519. Reports concerning intercepted wire, oral, or electronic communications | 301 |
| § 2520. Recovery of civil damages authorized | 302 |
| § 2521. Injunction against illegal interception | 303 |
| § 2701. Unlawful access to stored communications | 303 |
| § 2702. Disclosure of contents | 304 |
| § 2703. Requirements for governmental access | 305 |
| § 2704. Backup preservation | 307 |
| § 2705. Delayed notice | 308 |
| § 2706. Cost reimbursement | 310 |
| § 2707. Civil action | 311 |
| § 2708. Exclusivity of remedies | 311 |
| § 2709. Counterintelligence access to telephone toll and transactional records | 311 |
| § 2710. Definitions for chapter | 312 |

C *Computer Fraud and Abuse Act* **313**

| | |
|--|-----|
| §1030. Fraud and related activity in connection with computers | 313 |
|--|-----|