CYBERLAW FOR THE MASSES? A REVIEW OF *Netlaw: Your Rights in the Online World* by Lance Rose, Osborne McGraw-Hill, 1995

I. INTRODUCTION

For some of us, the online world is a scary place, full of uncertainty, rapid change and hidden perils to our privacy and pocketbooks. This is due in part to the perception of cyberspace as a lawless frontier where the usual rules don't apply. Do you really want to enter your credit card number into a strange website and click on the button entitled 'submit'? What would you do if, because of internet fraud, you are left staring at a phone bill for a 367 hour phone call to Moldova that you can't remember making?[1] Who is responsible and how do you sue them? If you are unable to bring an action in a foreign location, can you sue the system administrator who makes a fraudulent act possible? If so, how can honest system administrators tell if a fraudulent act is committed on their computer systems and thus protect themselves from litigation?

Obvious violations of law in the physical world become murkier in cyberspace. For example, in an online envronment it may not be clear precisely what constiutes slander or defamation.[2] The ease with which materials are copied, modified and transmitted produce difficulties in applying copyright statutes or enforcing remedies.[3] Existing laws will have to adapt to this new environment and new laws are needed to address problems that do not have obvious analogs in the physical world. For example, because of the borderless nature of cyberspace, traditional theories and methods of obtaining jurisdiction over a defendant may need to be expanded or reinterpreted.

Despite the perceived risk, the online world is still a relatively safe place for computer users and system operators. Generally, the gravest danger is an irrational fear of cyberspace. A modicum of basic legal knowledge can help to eliminate many irrational concerns and alert users and system operators to real dangers. Where there is real danger, it is usually possible to protect yourself and your clients with appropriate legal planning. Lance Rose's *NetLaw* attempts to cut through online

---

[1] In March 1997 this actually happened when a bogus online adult website defrauded hundreds of unwary users by creating a modem connection to Moldova that was left open causing very large telephone charges. *X-Rated Fraud Uses Internet to Bilk Users,* N.Y. Times, Feb. 20, 1997 at B1.

[2] *See* Daniel v. Dow Jones 137 Misc. 2d 94, 520 N.Y.S.2d 334 (1987) (comparing an online service to a print publication for the purposes of First Amendment analysis).

[3] *See* Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993) (holding that a computer bulletin board system that provided access to digitized magazine pictures without permission of the copyright owner were actionable under copyright law).

myths by clearly explaining what online hazards exist and how to protect against them. And, when the worst does materialize, *NetLaw* discusses what is illegal and who is responsible for illegal acts. *NetLaw* is thus an useful starting point for anyone who may have a legal concern related to the internet.

I. *NETLAW* FOR LAWYERS

As electronic services and electronic commerce expands, a wider range of lawyers are likely to encounter problems discussed in *NetLaw* in the course of their practices. *NetLaw* is nothing if not ambitious; Rose attempts to discuss free speech, contracts and commerce, ownership and use of online property, negligence and defamation, privacy, online crime, searches and seizures, and adult materials—a set of topics that might occupy a diligent law student for several years. Surprisingly, Rose manages to handle such a broad spectrum of technological and legal concepts in a useful and intelligent way in a mere 372 pages. Rose's treatments are accessible without oversimplification. Computer scientists, system operators and users of online services as well as experienced lawyers will find the practical information in this book useful.

Lawyers who have network service providers[4] as new clients will benefit from using *NetLaw* as a starting point. For instance, the appendix contains a number of sample contracts that raise issues faced by companies that sell access to the internet. Rose provides model contracts for transactions between network providers and the users of online services as well as contracts with the individuals who provide the programming content for the service. There is even a sample contract between the network service provider and independent companies who rent space to sell their products on the service.

The appendix also includes relevant portions of applicable stautory law such as the Electronics Communications Privacy Act,[5] and the Computer Fraud and Abuse Act[6] — necessary and useful information for a system operator desiring to stay within the boundaries of the law. In addition, portions of the New York Computer Crime Statute[7], First Amendment Privacy Protection[8], Child Pornography Statute[9] and FCC Restrictions on Obscene and Indecent Telephone Transmissions[10] are in-

---

4 Network service providers sell access to the internet to homes and businesses. Although there are several large service providers such as Compuserve and America Online, there are also thousands of small, often specialized, service providers.

5 18 U.S.C. §§ 2510-2521 (1994).

6 18 U.S.C. §1030 (1994).

7 N.Y. Penal Law §156.00 (Consol. 1992).

8 42 U.S.C. §2000aa-2000aa-12 (1994).

9 18 U.S.C.S. §2252 (1994).

10 47 U.S.C.S. §223 (1994).

cluded. Rose also provides a list of additional material including magazine articles, online resources, books, software, conferences and law review articles.

Rose uses case summaries and examples to make his points clear and understandable. He explains the risks of many online activities by analogizing to physical acts that are easier to grasp. Specific examples are set off in text boxes that are easy to review; this is particularly useful for those without legal training because the examples highlight situations that have been held to be illegal that the reader can compare to the activities they may be engaged in. The examples also illustrate how courts are struggling to place online activities into traditional legal frameworks, which offer a sense of continuity in the law while online problems inevitably stretch traditional legal doctrines into unrecognizable forms.

III. PRACTICAL ADVICE FOR THE ONLINE COMMUNITY

There are a number of summaries that give non-lawyers a sense of their legal rights and duties online. A service operator can get an overview of what actions to take if illegal or questionable activity on the operator's system is discovered. Since courts tend to treat the system operator as an active monitor responsible for policing the system, Rose recommends locking a user out of the system if the activity is harmful to another user. If the activity is illegal, he recomends reporting it to the police. In addition, the system operator is made aware that he or she can be held responsible if illegal activity on the system is reported to the operator or if the operator discovers the activity and fails to take corrective action.

Rose even provides legal guidelines for various online denizens, including moderators, node operators and online publishers. Again, he provides general guidelines that are intended to keep activities legal. Contracts, commercial law, negligence law, defamation law, copyright law and trademark law are discussed with an emphasis on their impact on those persons who are engaged in providing online services.

IV. NETPOLITICS: THE FUTURE OF ONLINE LAW

Rose is clearly worried about laws that might hamper online service providers. The first chapter spends nearly forty pages on First Amendment law, and Rose weaves First Amendment law into most of the later chapters. He argues that the First Amendment requires a great deal of protection for service providers from criminal and civil actions. He believes that too much interference is likely to have a chilling effect on service providers' ability to provide a forum for the discussion of public issues and diverse points of view. In this vein, Rose argues that the system operator should be immune from most actions and the user that is

directly responsible for the causing the act should be the party held responsible.

While this may certainly aid the system operator in avoiding liability, it may be difficult to hold a user liable or to collect a judgment. Also, system operators are no longer small operations; online service providers are becoming very large corporations. American Online (AOL) and the Microsoft Network (MSN) have the resources necessary to do a limited amounted of policing on their networks and may not deserve blanket immunity solely because they allow some political discussions and provide some news. Rose explains in great detail why the system operator deserves extensive protection from liability, but in the real world the economics of providing online services does not require this view.

V. CONCLUSION

NetLaw is particularly useful for the curious lawyer, computer affectionado, online service provider, or dilletante interested in the rapid development of online activities. Rose provides interesting insight into how the law is presently being applied to online activities, as well as discussing how it should evolve. He consistantly presents real world examples that make it easy for readers to understand how these legal concepts apply to everyday activities. Rose has done an admirable job of making an often jumbled caselaw into usable guidelines that everyone can understand and benefit from. As the online user community comtinues its exponential growth, it is virtually certain that an increase in lawsuits will follow. We recomend *NetLaw* with only one caveat: it will rapidly become dated in this fast-moving field.

Eric Smalley and John Greco†

† Eric Smalley, J.D., Cornell Law School, 1997. Jay Greco, candidate for J.D., Cornell Law School, 1998.