

ADR and Cyberspace: The Role of Alternative Dispute Resolution in Online Commerce, Intellectual Property and Defamation

E. CASEY LIDE

I. INTRODUCTION

The growth of digital networked communication has presented some troubling questions for the legal field. In some instances, the nature of the medium does not pose much of a problem; the application by analogy to existing legal principles is fairly clear.¹ Some issues arising from computer-mediated communication, however, are fundamentally new, with the novel and dynamic nature of the medium itself creating relationships unanticipated by a traditional, spatially-oriented body of law. The use and encouragement of alternative dispute resolution (ADR) methods could play a large and effective role in the adaptation process.

The dominant feature in the online landscape right now is the Internet, and most issues discussed in this Note will relate primarily to it.² The term "cyberspace," however, carries a more comprehensive meaning incorporating many types of digital networked communication, whether or not they rely on the Internet for execution, and apparently includes everything from satellites to cellular phones to computer bulletin board systems (BBSs). Naturally, the role of ADR in cyberspace will probably be greatest where there is a high degree of interactivity between a wide variety of users; at this point the Internet is the framework for such an environment.

ADR's role in the decentralized regulation of cyberspace will be discussed in three substantive contexts: (1) the commercialization of cyberspace, (2) intellectual property and (3) defamation. Within each context, some problematic legal application issues will be presented,³

¹ Some feel defamation law generally transfers well to digital communication. *See infra* note 82 and accompanying text.

² Two prominent subsets of the Internet, the World Wide Web and Usenet, are particularly relevant. With its graphical, point-and-click browsers, the World Wide Web has made a certain aspect of the Internet user-friendly. Usenet is an easily accessible collection of thousands of "newsgroups," which allows any user to post often lengthy comments in the collective discussion of the given topic. Usenet essentially gives each user his or her own printing press, allowing tremendous publicity without the filter of acceptance into a medium with a need for commercial success.

³ It must be emphasized that this Note is not devoted to a complete analysis of the individual legal questions themselves. The examples only serve to establish a premise that many of the troublesome applications of law are caused by the same factors which ADR has

followed by an evaluation of the ameliorative role ADR might play.⁴ This Note will conclude with a discussion of how ADR might be—and has been—implemented in the cyberspace context.⁵

Some recurring themes will become apparent. Often central to the question of traditional law's applicability in a given cyberspace-oriented instance, they also point to the relevance of ADR. The primary themes are:

- the importance of custom, and the recognition of its strong developing presence in cyberspace;
- jurisdictional concerns and other ramifications of an easily-accessible international medium;
- the dominance of contract doctrine in cyberspace jurisprudence;
- the significance of "dynamic routing"⁶ and the basic elusiveness of the medium to top-down regulatory control;
- the strength of ADR generally in related non-cyberspace areas (in international intellectual property disputes, for instance); and
- the rapid growth of technology, as both the cause of legal-application problems and as a source for self-regulatory solutions.

been proven to ameliorate, evidenced by the recent growth of ADR in some specific areas to be discussed.

⁴ This role which could range from an intermediate "stop-gap" measure, in lieu of reliance on an uncertain body of law, to the laying of the groundwork for a comprehensive system of decentralized regulation.

⁵ For the sake of simplicity, the actual implementation of ADR in a given context, whether it be through a contract to arbitrate, a court mandate or as the foundation of an international cyberspace dispute resolution framework, will not be discussed in great detail.

⁶ Information is not sent on the Internet with a designated path to reach its destination. There is simply a request that the information be passed along the various Internet-serving computers, or "nodes," until it reaches the desired computer hooked up to the Internet. If an attempt to pass it along fails, alternate routes will be tried until the information is successfully delivered, or until it is determined that access is unavailable. Because of this dynamic routing of information, and because no one computer system is essential to its operation, it is very difficult to regulate what happens on the Internet itself. See Andrew Grosso, *The National Information Infrastructure*, 41 FED. B. NEWS & J. 481, 481, 482 (1994).

In Ontario, officials instituted a gag order regarding a sensational murder case "to avoid an O.J. Simpson-like circus of publicity." The gag order effectively restrained mainstream media outlets, but was inert against the Internet. Someone created a Usenet group dedicated to the case and after users began posting news and rumors concerning the case, officials ordered Canadian systems operators to eliminate the group from their disks. The operators complied, but the Internet could easily be used to reach the newsgroup from other servers in the United States and elsewhere. See Edwin Diamond & Stephen Bates, *Law and Order Comes to Cyberspace*, TECH. REV., Oct. 1995, at 24, 27.

II. TROUBLESOME APPLICATIONS

A. *Online Commerce*

"Commerce on the Internet" encompasses a spectrum of definitions. Viewed simplistically, online commercial relationships could be categorized as one of a few types. The first is a detached retail relationship, with a consumer (user) interactively evaluating the product and perhaps making a purchase online. "Electronic malls," prominent on the World Wide Web, are an example of this. Second are the contractual relationships of individual users and specialized online institutions, such as banks facilitating the use of "digital cash." (This definition could perhaps be expanded to include a user-service provider relationship.) A third type involves actors with greater ability to bargain and more power over contractual terms. It could better be described as "conducting business" over the network and would entail using the medium more directly for any or all stages of negotiation, the exchange of contracts, the transfer of money and perhaps the transfer of the "goods" themselves if the commodity is information. Although commercial relationships on the Internet could be loosely described in terms of these three models, issues relating to the difficult application of law⁷ and the suitability of ADR are generally common to all three.

Of preeminent importance in this area is the recognition of custom, a concept with widespread implications in commercial law, particularly in international commercial law. Cyberspace is replete with customary ways of doing things; at an individual, e-mail and "chat" level, "netiquette" dictates the acceptable manners of online communication. As commerce increases on networks, custom will proliferate and develop on a larger, commercial scale and may, in fact, conflict with "real world" customs.⁸ ADR can be a means

⁷ Some might favor an approach to development of modern commercial law that requires fitting electronic practice and the law that governs it into . . . old paradigms developed for paper, hard goods and the other traditional venues around which commercial law was organized. But fitting new models into old forms takes too much from both. It limits the technology and technological evolution by forcing its conformance to frameworks developed to suit old technology or, failing that conformance, by offering an unsettled and perhaps inappropriate legal framework of outcomes respecting that technological practice. It also alters the old paradigms in ways that adversely affect their function even in the fields of their initial application.

Raymond T. Nimmer & Patricia Krauthouse, *Electronic Commerce: New Paradigms in Information Law*, 31 IDAHO L. REV. 937, 938-939 (1995).

⁸ See I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. PITT. L. REV. 993, 1009-1010 (1994).

to an accurate reflection of custom in the dispute resolution process and is especially suitable where expertise in a specific area is needed.

Custom and its impact on a dispute resolution process is exemplified in the Law Merchant, a historical concept with strong correlations to cyberspace.

The Law Merchant was a body of customary rules—the precursor to contemporary commercial law—that grew up in Medieval Europe as a response to the needs of international commerce

. . . .

. . . It was simply an enforceable set of customary practices that inured to the benefit of merchants, and that was reasonably uniform across all the jurisdictions involved in the trade fairs. Two key elements of the Law Merchant for our purposes were first, that no statute or other authoritative pronouncement of law gave rise to its existence, and second, that the Law Merchant existed in some sense apart from and in addition to the ordinary rules of law that applied to non-merchant transactions.

In other words, the Law Merchant made no attempt to displace existing rules promulgated by the jurisdiction in which a given trade fair might be held; it merely supplemented those rules with specific rules applicable to merchants' transactions The emphasis of these merchant courts and the law they applied was a speedy resolution of disputes, an important element when time is money. But another significant attribute of these courts was practicality and flexibility. Merchant practices were not static, and a reliance on local judges, taken from the merchants' own ranks and following the known customs of merchants, gave the Law Merchant an adaptability to changing times that statutory enactments would not have provided.

. . . .

The parallels with cyberspace are strong.⁹

In modern, online commerce, technological innovations will inevitably result in the development of customary practices. The same innovations may also challenge some of the basic presumptions on which existing commercial law is based.

⁹ *Id.* at 1019–1021.

A primary concern surrounding modern online commerce is security.¹⁰ Stories of hacker activity and the number of perceived security threats are common.¹¹ "Buyers and sellers must feel that transactions are secure, that the funds are moving to the proper place and that both parties to the transaction are who they say they are."¹² As an effort to meet the security needs of electronic commerce, digital cash¹³ and the Digital Signature Standard¹⁴ have seen much development. These and other technological innovations will have a powerful influence on the way business is done in cyberspace.

The context of Internet security is an excellent example demonstrating how such technological innovations can raise a number of legal application problems:

¹⁰ See Michael Rustad & Lori E. Eisensmidt, *The Commercial Law of Internet Security*, 10 HIGH TECH. L.J. 213 (1995).

¹¹ A recent electronic bulletin board service survey reported that 69% of the respondents' firms perceived significant security threats. Half of those respondents reported theft of property of \$10,000 or more. Around 18% of the respondents reported that their firm was victimized by fraudulent computer activity by a trusted party or insider. Approximately 10% reported fraudulent losses to outsiders. About 93% of the responding firms had implemented a network security project.

Id. at 216 (citing RICHARD H. BAKER, NETWORK SECURITY: HOW TO PLAN FOR IT & HOW TO ACHIEVE IT 183-184 (1995) (reporting survey of COMSEC BBS) (footnotes omitted)).

¹² Gerald Tebben, *Forum Sees Security as Barrier to Widespread Internet Use*, COLUMBUS DISPATCH, Oct. 1, 1995, at 2G.

¹³ In the basic form of digital cash, a financial institution creates a note that is then digitally signed using the institution's private encryption key. It withdraws the money from the customer's account (or otherwise charges the customer), and electronically transmits the note to the appropriate person. This note can then be electronically negotiated to others as payment for goods or services.

Grosso, *supra* note 6, at 484.

¹⁴ A digital signature uses encryption technology to satisfy the authentication requirement. A sequence of digits is appended to the end of an electronically transmitted document. "These digits are encrypted in such a way that, once decoded, the receiver is assured that only the desired sender was capable of encoding the sequence of digits in the form received." *Id.* at 483. However, adoption of standardized digital signature technology has several hurdles of its own before it comes into effect, including the de facto acceptance of an algorithm other than the one developed by the National Security Agency (NSA), a patent dispute, a possible flaw in the algorithm, and Clipper Chip-inspired concerns over the motives behind the NSA algorithm. See *id.* at 483-484.

A large number of network security products have recently appeared on the market which claim to have solutions to the problem of the "Bad Internet." One new security product was described as "close to the level of "bullet proof". [sic] Some firms have even represented their products to be "hacker-proof." Because of the lag between the legal infrastructure and the new network security technologies, it is completely uncertain whether representations such as these would be deemed enforceable by a court of law.¹⁵

....

... Common law negligence does not define a level of care for Internet security providers, and ambiguities result when the historical means of establishing such a standard are employed. Moreover, no statute has been enacted to define Internet security standards. The application of negligence doctrine to the business of providing on-line services highlights these open questions and exemplifies why current negligence theory is ill-equipped to deal with Internet security liability.¹⁶

Currently, most users of the commercial Electronic Data Interchange (EDI)¹⁷ do not allocate risk and establish ground rules in separate paper trading partner agreements.¹⁸ "The EDI data as encoded is not designed for the exchange of textual material such as terms and conditions clauses."¹⁹ A recent Model Trading Partner Agreement is designed to be a one-time written agreement between partners, which establishes "the meaning, timing, interaction and responsibilities arising from electronic messages and sets forth the legal import of a particular transaction between the trading partners."²⁰ Such an all-inclusive agreement is liable to be the subject of many disputes and contains a suggested arbitration clause.²¹

¹⁵ Rustad & Eisenschmidt, *supra* note 10, at 217-218.

¹⁶ *Id.* at 245.

¹⁷ "EDI is the method by which business data may be communicated electronically between computers in standardized formats (such as purchase orders, invoices, shipping notices, and remittance advices)." John C. Yates, *Recent Legal Issues in Electronic Commerce and Electronic Data Interchange*, at 271 (PLI Pat. Copyrights Trademarks & Literary Prop. Course Handbook Series No. 430, 1996); *The Commercial Use of Electronic Data Interchange—A Report and Model Trading Partner Agreement*, The Electronic Messaging Services Task Force.

¹⁸ See Yates, *supra* note 17, at 290.

¹⁹ *Id.*

²⁰ See The Electronic Messaging Services Task Force, *supra* note 17, at 1645.

²¹ See *id.* The Model Trading Partner Agreement was prepared by the Electronic Messaging Services Task Force of the American Bar Association Subcommittee on Electronic Commercial Practices. See The Electronic Messaging Services Task Force, *supra* note 17, at

In less formal, individual-level business relationships of cyberspace, "strangers need to be able to deal with each other electronically without negotiating paper trading partner agreements."²² Like the above contexts of Internet security and large-scale commercial trading partner agreements, the development of the "pluralistic electronic market" will be accompanied by the further establishment and formalization of custom for a primary reason: dynamic technological development creates difficulties in the predictable application of traditional commercial law.

U.C.C. provisions which support the reflection of custom will be important: "As sales of goods become more common via the NII [National Information Infrastructure], the U.C.C. will likely become more useful based on the flexible 'course of dealing' and 'usage of trade' definitions."²³ But the new technology designed to facilitate electronic commerce also raises questions regarding the U.C.C., in particular, issues of contract formation, receipt and verification and the statute of frauds.²⁴ Some scholars feel the problem is a fundamental one:

The problem with the U.C.C. is the basic assumption that commercial transactions are conducted on paper. In a world where contract terms and even signatures may be made of electronic impulses rather than pen and ink, the union of the U.C.C.'s more arcane provisions and computer technology has been a rocky marriage at best.

....

... [B]ecause computer generated commercial transactions are not consistently protected by the courts, new means of conducting business are not effectively protected through the U.C.C. or the common law as currently applied by many jurists who do not, or choose not, to understand the technology and how the technology interacts with the purpose of the applicable law.²⁵

1697.

²² Henry H. Perritt, Jr., *President Clinton's National Information Infrastructure Initiative: Community Regained?*, 69 CHI.-KENT L. REV. 991, 1007 (1994).

²³ BRUCE A. LEHMAN, INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE 57 (1995).

²⁴ See Gregory E. Perry & Cherie Ballard, *A Chip by Any Other Name Would Still Be a Potato: The Failure of Law and its Definitions to Keep Pace with Computer Technology*, 24 TEX. TECH L. REV. 797, 823 (1993).

²⁵ *Id.* at 824-826.

Even though the proposed U.C.C. Article 2B will undoubtedly clarify the situation by eliminating some strained legal fictions,²⁶ commentators continue to note the desirability of a "uniform commercial law of the Internet."²⁷

Rather than rely on an uncertain and unpredictable body of law which in several ways has not yet adapted to technological developments, effective dispute resolution may be found in arbitration or mediation, with a neutral party versed in the subject and familiar with the customs of the cyberspace commercial community. Such a tribunal would be particularly useful in situations where traditional law calls for a determination of "reasonableness." As the development of digital communication—and custom—continues to challenge the adaptability of law, the need for a more flexible method of dispute resolution will increase.

In addition to being a system of dispute resolution flexible enough to accommodate an extremely dynamic area, a primary strength of ADR here is its recent acceptance into commercial disputes generally. A strong incentive for the use of ADR in commercial disputes, with obvious relevance to cyberspace, is the opportunity to avoid potential jurisdiction problems. Parties can develop arbitration agreements which stipulate their choice of law, eliminating potential delays which may result from a dispute over jurisdiction.

The jurisdiction problem is considered by some to be *the* problem of the Internet. Is a virtual presence sufficient to establish personal jurisdiction? When people make information available over the Internet, have they subjected themselves to suit everywhere that information can be accessed? Recent court cases concerning Internet jurisdiction offer little guidance, and some appear to be dodging the issue.²⁸

²⁶ See Rustad & Eisenschmidt, *supra* note 10, at 300.

²⁷ "A uniform commercial law of the Internet that applies no matter where the parties reside must be formulated. It should remove barriers to trade and facilitate commercial transactions across the Internet." *Id.* at 298.

²⁸ The Sixth Circuit recently decided *CompuServe, Inc. v. Patterson*, 89 F.3d 1257 (6th Cir. 1996), a case involving the question of whether electronic contacts are sufficient to support the exercise of personal jurisdiction. The defendant is a CompuServe subscriber who had signed a contract with CompuServe, based in Ohio, allowing him to sell shareware over the system and also providing that it was subject to Ohio law. The defendant sold a small amount of shareware to twelve CompuServe subscribers in Ohio, but he had never been to Ohio himself. Using highly fact-specific reasoning, the Sixth Circuit held that jurisdiction based on his distribution of shareware was appropriate, but expressly stated that it was *not* deciding whether the defendant would be subject to jurisdiction in every state in which the defendant's shareware was purchased or used.

The courts in general have strongly supported the expansion of ADR. "Courts may potentially scrutinize ADR at any one of three stages: agreements to arbitrate or mediate; the proceedings themselves; or the resulting awards or settlements. In all three areas, recent decisions have further limited the grounds for judicial review."²⁹ This is especially true in contractual arbitration.³⁰

The flexibility, speed and general commercial acceptance of ADR strongly suggest it will have a prominent role in the development of digital commerce. As a method of dispute resolution which can reflect developing custom and account for developing technology with little danger of stifling either one, ADR could be a valuable tool in an environment where the law is struggling to adapt.

B. Intellectual Property

The development of digital communication has produced, and will continue to produce, novel intellectual property issues.³¹ Many of these issues will no doubt be resolved via analogy to existing law, or perhaps after some minor tinkering.³² But in some cases, the nature of the medium—

²⁹ S. Gale Dick, *ADR at the Crossroads*, DISP. RESOL. J., March 1994, at 47, 52.

³⁰ *See id.*

³¹ With developers now using the Internet to distribute software on a subscription basis and users incorporating software from the Internet into new commercial products, thorny intellectual property issues arise, such as who owns works and their improvements that, like boundless ideas, can be instantly reproduced, in whole or part, and globally distributed?

Kristi L. Vaiden, *Software on the Internet: Intellectual Property Challenges*, ACCA DOCKET, Jan.–Feb. 1995, at 56, 56.

"Say that a New York City user downloads a favorite Sherlock Holmes story from a London computer. The works of Arthur Conan Doyle are in the public domain in the United Kingdom but some are still under copyright in the United States. Which country's law prevails?" Diamond & Bates, *supra* note 6, at 26.

³² A World Intellectual Property Organization (WIPO) committee and a U.S. working group rejected "the premise that 'intellectual property cannot be patched, retrofitted or expanded to contain the gases of digitized expression.'" Barbara Hoffman, *Digital Innovations Now Challenge Legal System*, NAT'L L.J., Oct. 23, 1995, at C15 (quoting John Perry Barlow, *The Economy of Ideas: Everything You Know About Intellectual Property Law Is Wrong*, WIRED, March 1994, at 84, 85). As discussed *infra* notes 38–41 and accompanying text, the U.S. working group concluded that uploading and downloading constituted "copying" for the purposes of the Copyright Act of 1976. Even if this is an accurate interpretation of the word copying for the Copyright Act, it is an interpretation that, by the nature of the statute

digital, storable, instantaneous, global and elusive—seems to produce a very new question.³³ The use of ADR can be a rational choice flexible enough to accommodate a rapidly changing technological medium.

The status of the system administrator promises to be a difficult issue in online copyright cases. In *Playboy Enterprises, Inc. v. Frena*,³⁴ a small, private BBS (Bulletin Board Service) was found liable for copyright infringement. The BBS provided a file-sharing service; users send files to the BBS which can then be downloaded, or copied, by other users.³⁵ In the *Playboy* case, Playboy asserted copyright to photographs that existed in the BBS's file sharing service. The system administrator claimed he was unaware of the existence of the photographs, but the court held that scienter was not an essential element and decided in favor of Playboy on a summary judgment motion.³⁶

It is quite true that scienter is not a normal requirement of copyright infringement. Yet this case will trouble many cyberspace users. It certainly will trouble system administrators, for it seems to impose a near-impossible burden on them to screen all uploaded files. Many BBS systems experience hundreds of such uploads daily.³⁷

(designed for a different medium where duplication is more difficult), competes with the fundamental mechanics of the Internet, which *functions* by copying.

³³ At a shallow level of analysis, every new medium is fraught with complex new legal questions, the most fundamental among them being whether existing laws designed with other media in mind should be applied to the new medium as well. On the other hand, at the deepest or most general level of analysis, no legal questions are unique: they all involve human conflict. The trick is knowing when to take a shallower and when a deeper view.

Hardy, *supra* note 8, at 996.

³⁴ 839 F. Supp. 1552 (M.D. Fla. 1993). Another case, scheduled for trial in the spring of 1996, involves a suit by the Church of Scientology against an Internet service provider and will decide its liability for contributory copyright infringement in the context of a potential fair-use defense. See *Religious Technology Ctr. v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995) (denying motions for summary judgment and judgment on the pleadings).

³⁵ See Hardy, *supra* note 8, at 1002.

³⁶ See *id.*

³⁷ *Id.*

The volume of uploads and downloads, the ease of copying, and the wide array of copyrightable materials that can travel in cyberspace, all make BBS administrators poorly suited to the standards of "knew or ought to have known" about the copyright

In the recording industry, performance rights are called into question.³⁸ The Copyright Act of 1976 confers various rights on music publishers and recording artists, but those rights have not been delineated in cyberspace.³⁹ Performance licenses, mechanical licenses and synchronization licenses are easily applied to the tangible and analog world for which they were created, but digital communication has caused confusion.⁴⁰ For the payment of royalties, questions of duplication are central, and the nature of digital, computerized communication in which a storable, easily-transferred pattern of bits can constitute a copyrighted work⁴¹ has caused a gap between existing law and the policies which it seeks to promote.

The Copyright Act of 1976 is central to the domestic digital communication-copyright debate and is subject to some changes.⁴² Notably, a U.S. working group recommending alterations to the Act came to a conclusion that implicates the very nature of computerized, networked communication as "copying" for the purposes of copyright law.⁴³

status of information held on their systems. Unlike a bar or club where music is played, system administrators cannot know in any general sense whether or not the files being up- and down-loaded from their systems should be treated with the gingerliness appropriate for commercially valuable copyrighted materials.

. . . [T]he role of the system administrator with regard to uploaded copyright-infringing materials seems different from real space analogs and hence "new" enough to be worthy of further attention.

Id. at 1007-1008.

³⁸ See Seyamack Kouretchian, *Digital Pirates Are Plundering Performance Rights*, NAT'L L.J., Oct. 23, 1995, at C12.

³⁹ See *id.* (citing 17 U.S.C. §§ 101-1010 (1994)). In November 1995, Congress passed the Digital Performance Rights in Sound Recordings Act (17 U.S.C. § 106). The statute creates a limited performance right for the owner of a sound recording copyright, but its application may be limited to subscription digital audio services.

⁴⁰ "The Copyright Act has been legislatively written and judicially interpreted to apply to . . . tangible and analog situations. Many of these statutory rights, however, are blurred—if not entirely lost—in the digital world of modems, multiservers and interactive on-demand downloading." *Id.* at C12.

⁴¹ Although it presently takes fifty minutes to transfer one minute of CD-stereo quality audio via a 14.4-kilobit-per-second modem, the day soon will arrive when an entire album can be transferred in seconds. When this happens, the face of the recording industry will change, as will the royalties received by artists, publishers and labels.

Id.

⁴² See Hoffman, *supra* note 32.

⁴³ See LEHMAN, *supra* note 23, at 28.

A simultaneous fixation (or any other fixation) meets the requirements if its embodiment in a copy . . . is "sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration." . . . Electronic network transmissions from one computer to another, such as e-mail, may only reside on each computer in RAM (random access memory), but that has been found to be a sufficient fixation.⁴⁴

This definition includes uploading and downloading.⁴⁵ In a medium which *functions* by "copying," this determination promises to have widespread effect.

The fair use doctrine might raise some questions. Courts have noted that fair use should be adapted to technological innovations and that it is based on the author's implied consent to "reasonable and customary" use.⁴⁶ Also, second and third copies made by Web-site visitors (the first being the perusal of the information) for purposes of easier reading and to reduce online connection fees may constitute fair use.⁴⁷

The Copyright Act of 1976 ultimately may be a source of strong *domestic* protection for owners of copyrighted material because of its broad, powerful prohibitions against unauthorized "reproduction," "distribution" and "performance" contained in Section 106.⁴⁸ "The legal system is far less clear, however, once one passes beyond the U.S. borders."⁴⁹ Internationally, concepts of property and copyright vary considerably:⁵⁰

⁴⁴ *Id.* (quoting 17 U.S.C. § 101 (1988) (definition of "fixed")).

⁴⁵ See John B. Kennedy & Shoshana R. Davids, *Web-Site Agreements Do Not Wrap Up IP Rights*, NAT'L L.J. Oct. 23, 1995, at C3.

⁴⁶ See *id.* at C4.

⁴⁷ See *id.*

⁴⁸ See George Vradenburg, *When Law Alone Isn't Enough*, NAT'L L.J., Oct. 23, 1995, at C9, C10-C11.

⁴⁹ *Id.* at C11.

For example, it is not clear what action can be taken against a hacker located outside the United States who obtains unauthorized access to a U.S. data base and electronically copies and retransmits a motion picture entirely outside this country.

. . . [M]uch needs to be done in the international arena to develop effective legal remedies against international electronic infringement.

Id.

⁵⁰ See Jennifer A. Mills, Note, *Alternative Dispute Resolution in International Intellectual Property Disputes*, 11 OHIO ST. J. ON DISP. RESOL. 227, 229-230 (1996).

On an international scale, the difference affects the fundamental question of whether any property right exists and whether it can be transferred. This is largely uncharted territory for legal analysis. Consider, for example, a packet of data obtained by a Boston company from a German database through a remote access which passes through a Mexican computer. If the data is purely factual materials, and the EU Directive [adopting a "reciprocity" policy for the protection of international intellectual property (IP) rights] had been implemented, the German company "owned" a right to prevent or control extraction of the material from its database. On the other hand, in the United States, a principle of national treatment would indicate that no rights exist in a purely factual database. The circumstances in Mexico might fit either model or a third one. Has an infringement occurred? Under which set of laws will it be litigated?⁵¹

On an international level, the problem of copyright and digital communication is being debated under the aegis of the World Intellectual Property Organization (WIPO). The WIPO (which operates an intellectual property Arbitration Centre in Geneva) has convened a Committee of Experts on a Possible Protocol to the Berne Convention concerning developments since 1971, as well as a Committee of Experts on a Possible New Instrument for the Protection of Performers and Producers of Phonograms.⁵² The European Community and Canada have also produced reports.⁵³ A consensus among the reports seems to be that fundamental copyright concepts, based on tangible or analog forms of property, are sound; there is simply an application problem that eventually can be worked out with international cooperation. But even with faith in the continued applicability of historical concepts of copyright, the reports appear to be strongly in favor of employing technological means to protect intellectual property and, in fact, discussed the possibility of banning certain anti-

⁵¹ Raymond T. Nimmer, *Licensing on the Global Information Infrastructure: Disharmony in Cyberspace*, 16 NW. J. INT'L L. & BUS. 224, 231 (1995).

While the Berne Convention adopts an aggressive national treatment position, several recent enactments or proposals in the United States and in the EU adopt a reciprocity framework, presumably as a wedge to encourage other countries to follow the policy decisions reached in the country adopting the idea of reciprocity.

Id. at 230.

⁵² See Hoffman, *supra* note 32, at C15. See *infra* note 66-69 and accompanying text for discussion of the World Intellectual Property Organization and the WIPO Arbitration Centre.

⁵³ See Hoffman, *supra* note 32, at C15.

encryption software devices.⁵⁴

For now at least, the protection of intellectual property in cyberspace cannot rely solely on the threat of civil or criminal sanctions.⁵⁵ Several reactions could become even more apparent: (1) an increased use of technology as a means of protection; (2) the development of custom and (3) application of ADR principles.

Technology itself plays an increasingly important role in the protection of intellectual property.⁵⁶ With the unprecedented ease of duplication in cyberspace, intellectual property in a digital form faces a constant threat of widespread infringement. The ideal system of intellectual property protection would be effective against both unintentional, non-commercial infringers, as well as digital pirates with an intent to make money through reproduction. The development of encryption technology will be one means of protection, but other possibilities exist. A form of digital watermarking could provide a means of determining ownership. Automatic metering systems and automatic debit systems currently in development will be other powerful tools for protection.⁵⁷

Rather than completely eliminate the possibility of piracy, self-help technological techniques aim "to force the economics of commercial piracy to the point at which it can be profitable only on such a large scale that it will become visible to law enforcement and thereby vulnerable to criminal prosecution."⁵⁸ A comprehensive system of technological intellectual property protection "would depend on the development of standards, protocols and systems that transcend various platforms, technologies and national boundaries. . . . [E]xisting international legal systems and current-day technological systems are each, in themselves, inadequate. Both law and technology will be needed to address the problem of unauthorized

⁵⁴ See Robert A. Cinque, Note, *Making Cyberspace Safe for Copyright: The Protection of Electronic Works in a Protocol to the Berne Convention*, 18 *FORDHAM INT'L L.J.* 1258, 1271 (1995).

⁵⁵ See Vradenburg, *supra* note 48, at C9.

Now that digital copying and retransmission have made infringement far easier and far more damaging, authors and other copyright owners must look to scientists and engineers to assist them in protecting their products. The law no longer is enough. In today's world, it is impossible to protect intellectual property without the use of both law and technology.

Id.

⁵⁶ *See id.*

⁵⁷ *See id.* at C11.

⁵⁸ *Id.* at C10.

exploitation of intellectual property.”⁵⁹

As in the commercial context, cyberspace custom may play a large role in the development of intellectual property “cyber-law.” Based on the U.S. working paper mentioned earlier which included uploading and downloading as copying for the purposes of traditional copyright law, the Internet is essentially a huge morass of copyright violations. Every duplication, through uploading and downloading, of any material from any computer on the Internet has a strong chance of technically being a copyright violation; this is custom developing in direct contradiction to the existing law.

[W]e can look at the well recognized cyberspace custom of copying e-mail messages and forwarding them to others. In real space, this might be a clear copyright violation, but if everyone in cyberspace “does it all the time,” and knows that others do it all the time, might not some sort of estoppel or implied waiver of copyright rights arise?⁶⁰

Another specific example of developing custom can be found in the aforementioned recording industry. Performance-right societies (such as BMI and ASCAP) and online-system operators have begun developing a course of conduct that may become the industry standard.⁶¹ The performance-right societies “have begun enforcing their rights in cyberspace by demanding and receiving licenses from online-system operators using their repertoire over the Internet. This practical way of handling performance rights in the online community so far has helped to avoid precedent-setting lawsuits.”⁶²

In conjunction with the recognition that cyberspace custom is often incongruent with “real space,” the utilization of ADR is a natural extension from its already-prominent use in intellectual property disputes. While the general use of ADR has increased dramatically,⁶³ its development in intellectual property has been especially pronounced.⁶⁴ As in the above commercial context, the strength of ADR in the intellectual property (IP) practice area itself in many ways parallels its suitability for networked communication. In addition, the choice to arbitrate has been firmly supported by the courts.⁶⁵

⁵⁹ *Id.* at C11.

⁶⁰ Hardy, *supra* note 8, at 1009.

⁶¹ See Kouretchian, *supra* note 38, at C12.

⁶² *Id.*

⁶³ See Dick, *supra* note 29, at 47.

⁶⁴ See *id.* at 48.

⁶⁵ See Keith Highet & George Kahale III, *International Decisions*, 87 AM. J. INT’L L.

Recent trade agreements addressing intellectual property issues will cause an increase in the use of ADR for international IP disputes.⁶⁶ The WIPO has opened the WIPO Arbitration Centre in Geneva to offer dispute settlement services for private, international IP disputes.⁶⁷ In addition to eliminating a jurisdiction and choice-of-law question, ADR also offers a very flexible tribunal, necessary to accommodate the various international concepts of property.⁶⁸

Rather than spend large amounts of money unpredictably educating a judge or jury about a complex technological issue and hoping they empathize, many parties choose ADR as an opportunity to have the case decided by neutrals already versed in the subject and customs of the matter at hand. When technological development may have simply outpaced the law's ability to resolve disputes efficiently and effectively,⁶⁹ ADR may be preferred as an alternative to the litigation.⁷⁰

Arbitration has already been used to resolve a few Internet-related IP disputes. In trademark, a three-person, mutually-agreed-upon arbitral panel recently disallowed the use of another's registered name as an Internet domain address.⁷¹ While the case has no legal precedential value, it has produced much comment and will likely serve as guidance in related disputes. Technology-related trademark cases as a whole are still inconsistent: "Solutions, unfortunately, aren't found in law, they're found in arbitration."⁷²

282, 292 (1993). "There is no doubt that a U.S. district court may dismiss an intellectual property infringement action where a valid agreement to arbitrate exists." *Id.* at 294.

⁶⁶ See General Agreement on Tariffs and Trade: Final Act Embodying the Results of the Uruguay Round of Multilateral Trade Negotiations, (April 15, 1994) Annex 2.

⁶⁷ See Mills, *supra* note 50, at 235.

⁶⁸ See *id.* at 230, 239.

⁶⁹ "The rate of technological change has outstripped the ability of the law, lurching from one precedent to another, to address new realities. . . . Novel communications are pressed into service while still in their infancy, and the legal system's initial encounters with these newborns often have a lasting influence." LAURENCE H. TRIBE, *AMERICAN CONSTITUTIONAL LAW* §§ 12-25, at 1007 (2d ed. 1988).

⁷⁰ See *infra* notes 77-81 and accompanying text (discussing *IBM v. Fujitsu* and employment of ADR method of "preventative law").

⁷¹ See André Brunel, *Billions Registered, but No Rules: The Scope of Trademark Protection for Internet Domain Names*, J. PROPRIETARY RTS., Mar. 1995, at 2, 3-4.

⁷² *Id.*

Patent disputes focusing on the tools for the creation of the global information infrastructure will also increasingly use ADR: "The prevalence of such newly-developed, highly-technical inventions will increase the likelihood of patent disputes, and the value of resolution through arbitration."⁷³ Other reasons cited for the inclusion of ADR here include the opportunity for mutually-agreed-upon expert neutrals and the ability to stipulate choice-of-law questions.⁷⁴ In the always-changing high-tech patent industry, timing is often extremely valuable, making quicker resolution of disputes through arbitration valuable.⁷⁵ Faced with the unpredictability and inflexibility of litigation, IP parties may find that ADR can determine the applicable law between parties, enabling a flexible, trade-based approach that may even protect and facilitate development until the law becomes more settled and more predictable.⁷⁶

A recent high-profile computer software dispute exemplifies this problem of technological development and pressures of a dynamic market drastically outpacing law⁷⁷ and was settled successfully through a flexible arbitration (which also, to a large degree, dictated the parties' relationship for the future). While not directly implicating digital networked communication, the dispute involved many similar considerations, and its use of "preventative law" may offer some guidance as an effective resolution of high-tech disputes in general and cyberspace-related disputes specifically. In the 1982 IBM-Fujitsu dispute, IBM claimed that Fujitsu, which makes IBM-compatible hardware and software, had violated IBM's software copyrights.⁷⁸ Senior officials from each company spent eight months negotiating a settlement. In 1985, the companies used ADR to dictate a significant portion of their future relationship.⁷⁹ The agreement established a

⁷³ Karl P. Kilb, *Arbitration of Patent Disputes: An Important Option in the Age of Information Technology*, 4 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 599, 599 (1993). "The inevitable interaction of different information technologies in creating the 'information superhighway' will increase the potential for disputes involving a growing number of special inventions and designs." *Id.* at 611.

⁷⁴ *See id.*

⁷⁵ *See id.*

⁷⁶ *See Bar Meeting Explores Use of Alternative Dispute Resolution in Patent Disputes*, 39 Pat. Trademark & Copyright J. (BNA) No. 957, at 74, (Nov. 23, 1989).

⁷⁷ In terms of both the law's adaptability, and the need for a speedy resolution.

⁷⁸ *See* Ronald L. Johnston, *Alternate Dispute Resolution*, at 159 (PLI Pat. Copyrights Trademarks & Literary Prop. Course Handbook Series No. 369, 1993).

⁷⁹ *See* Kilb, *supra* note 73, at 615.

“Security Facility Regime,” under which each company can examine, under elaborate safeguards, certain parts of the other company’s software. In return for what is determined to be adequate compensation, the examining party could use the obtained information in developing its own software, and be assured of immunity from claims of copyright violations.⁸⁰

The settlement reached in the IBM-Fujitsu dispute incorporated an aspect of ADR known as “preventative law”:

Preventative law provides a unique advantage as a means of settling complicated issues in evolving technological and legal fields. In the past, . . . IBM had to wait until after the public release of a Fujitsu program and then conduct an elaborate technical examination of the program. Then, if it chose to pursue a claim, it was extremely expensive and time-consuming. Meanwhile, of course, the Fujitsu program at issue was already in the marketplace. [This preventative law] exposes and resolves disagreements before public release of the software.⁸¹

Intellectual property law must adapt to a global medium in which widespread duplication can be nearly instantaneous. The employment of ADR methods for cyberspace IP concerns is a natural extension from its already-prominent use in traditional IP disputes. Given the rapid development of technology (with new and better ways to infringe—and protect—intellectual property rights), a flexible method of dispute resolution such as ADR can be more appropriate than reliance on a relatively static body of traditional law.

C. Defamation

Disputes relating to defamation traditionally do not implicate conventional ADR methods (such as arbitration) to the same degree as in the commercial and IP contexts. But ADR could have a large role in cyberspace libel disputes, perhaps more so than in traditional libel cases. Again, this section will discuss some troublesome applications of traditional defamation law to cyberspace and will note some potential decentralized solutions.

⁸⁰ *Id.*

⁸¹ *Id.* (statement by Professor Robert Mnookin, an ADR specialist at Stanford University and one of the neutral experts in the IBM-Fujitsu dispute).

The broad concepts of defamation law generally transfer easily to cyberspace.⁸² But there are some substantial unanswered questions. The determination of what constitutes a “public figure” in cyberspace is far from clear, and, once again, the role and liability of the system operator is a major question. The global nature of the medium raises serious jurisdictional and substantive issues; the Constitution is, after all, a local document. With the ease of publication in cyberspace, a vindication-based remedy could become more prominent, perhaps supported by ADR processes which more accurately reflect the realities and customs of global computer-mediated communication.

American defamation law itself is cumbersome and complex.⁸³ When applied to cyberspace, it becomes especially murky. *New York Times Co. v. Sullivan*⁸⁴ and its progeny⁸⁵ established a framework based on whether the defamed is a “public figure”: if he is found to be so, the plaintiff must show that the utterance was made with “actual malice,” that is, with knowledge of falsity or with reckless disregard for the truth. The public figure determination, central to much defamation law, has called for the evaluation of up to nine different factors, according to one commentator.⁸⁶ Of particular significance in cyberspace controversies⁸⁷ are the traditional

⁸² Suppose a cyberspace user writes a defamatory message about another user and intentionally sends it over the Internet to a dozen other individuals. Is this situation materially different from sending the same message by fax, mail, or telegraph? It is hard to see how it could be.

... When cyberspace is simply a medium of direct communication between people—much like the telephone, mail or fax—we should expect that the legal issues will not be materially different from issues in “real” space.

Hardy, *supra* note 8, at 999–1000.

⁸³ The present “Constitutionalized” law . . . is a labyrinthine structure, similar to the ancient cosmology of epicycles, impairing predictability and leaving the field to a few priestly experts. [The cases] leave one acutely aware both of the difficulty of fashioning coherent doctrine in the context of the tension of the competing interests and of the need ultimately for a simpler structure.

SHELDON W. HALPERN, *THE LAW OF DEFAMATION, PRIVACY, PUBLICITY, AND MORAL RIGHT* 4 (2d ed. 1993).

⁸⁴ 376 U.S. 254 (1964).

⁸⁵ See generally *Gertz v. Robert Welch, Inc.*, 418 U.S. 323 (1974); *Curtis Publishing Co. v. Butts*, 388 U.S. 130 (1967).

⁸⁶ See RODNEY A. SMOLLA, *LAW OF DEFAMATION* § 2.09(4), at 2–33 (1994).

⁸⁷ See Thomas D. Brooks, *Catching Jellyfish in the Internet: The Public-Figure Doctrine and Defamation on Computer Bulletin Boards*, 21 *RUTGERS COMPUTER & TECH. L.J.* 461,

factors of (1) access to the media;⁸⁸ (2) existence of a public controversy and (3) the plaintiff's imposition into the controversy.⁸⁹

The public figure determination for many potential cyberspace defamation cases is, at best, unpredictable.⁹⁰ Given the increasing ease of access to the Internet; the proliferation, diversity and content of Usenet-type newsgroups⁹¹ and the potential audience for a single (perhaps careless) utterance, other ingredients of defamation law, may, at some point, face reevaluation as well.

The liability of a BBS operator is another major problem. If a user posts a defamatory message on a BBS, is the BBS liable as an intermediary? In *Cubby, Inc. v. CompuServe, Inc.*⁹² the court analogized CompuServe to a bookstore, finding no duty to screen or remove the defamatory utterance.⁹³

479 (1995) (citing RODNEY A. SMOLLA, LAW OF DEFAMATION § 2.09(4), at 2-33 (1994)).

⁸⁸ The U.S. Supreme Court has been reluctant to define "the media":

[The Court's] approach is reminiscent of that employed by Justice Stewart when faced with the task of defining pornography: the justices know it when they see it. In this manner, the Court finds defendants to be media parties or non-media parties without discussion. Relying expressly on whether a defendant was part of the media would confront the Court with the slippery-slope task of defining 'the media.' . . . [T]he Court continues to employ an ambiguous standard.

Brooks, *supra* note 87, at 478-479.

⁸⁹ See *id.* at 479.

⁹⁰ Advertisers on the Internet face additional concerns: "The trend is that courts are generally willing to find that a plaintiff has voluntarily injected himself into a controversy when he makes use of advertising." Brooks, *supra* note 87, at 471.

⁹¹ The Supreme Court has held that issues that are newsworthy, titillating, or of general public concern do not merit classification as public controversies for purposes of the public-figure doctrine. Such issues, however, are currently the bread and butter of most online bulletin boards and news groups. Thus, those who post messages to such boards or groups seem unlikely to be faced with the prospect of proving actual malice if defamed. So, for example, participants in news groups devoted to discussing, say, the O.J. Simpson trial, Michael Jackson's marriage to Lisa Marie Presley, or GATT, will have to show only that a defendant's allegedly defamatory statement was made negligently.

Brooks, *supra* note 87, at 485.

⁹² 776 F. Supp. 135 (S.D.N.Y. 1991).

⁹³ If a BBS purports to exercise some degree of editorial control over postings, it may open itself up to liability. In *Stratton Oakmont, Inc. v. Prodigy Services, Inc.*, 63 U.S.L.W. 2765 (N.Y. Sup. Ct. 1995), a New York trial court found Prodigy, a large commercial BBS, liable for a defamatory statement on its service. Prodigy markets itself as a family BBS and

The conclusion and the analogy were based largely on practicality. “[L]arge commercial BBSs like Prodigy and America OnLine [sic] serve as the mail box for thousands of messages a day; it is not feasible for those companies to examine every message.”⁹⁴

But there are several reasons why the bookstore analogy may not serve as a blanket precedent relieving all BBSs from intermediary liability:

The policies behind relieving “real space” intermediaries of defamation liability are not clearly applicable in cyberspace, or at least not uniformly applicable because (1) the practicalities of screening messages for defamatory content differ from BBS to BBS; (2) the value of intermediaries [bookstores, for instance] in real space situations is far more well established than the value of on-line intermediaries; (3) those intermediaries in real space that are common carriers have made trade-offs in the form of universal carriage and often monopoly positions that cyberspace system administrators do not typically make; and finally, (4) solvent publishers as potential defendants are more likely to exist in real space intermediary situations than in cyberspace. The applicable legal rules of defamation . . . surrounding the system administrator as intermediary are therefore sufficiently uncertain to make them “new” enough to merit attention.⁹⁵

Another factor sure to cloud the application of defamation law to cyberspace is the vastly increased ability to communicate internationally. A reflection of the Internet’s global nature, most network fora, such as Usenet, are not at all limited to the United States. Online communication transcends national boundaries and can be had with citizens of Australia or Europe just as easily and cheaply as with citizens of one’s own country. “The extremely low cost of cyberspace communication makes practical the distribution of defamatory or other wrongful communications on a scale not before possible. For these reasons, the issue of international torts is likely to

actively screens obscene and offensive messages. See Richard Raysman & Peter Brown, *On-Line Legal Issues*, N.Y.L.J., Feb. 15, 1995, at 3. “If Prodigy were held to be liable because it exercised editorial control, that outcome might force other on-line service providers to the extreme position of relinquishing any control over their electronic bulletin boards, which, in turn, may transform the Internet into a fertile ground for defamation and libel.” *Id.*

⁹⁴ Hardy, *supra* note 8, at 1003 (citing *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135, 140 (S.D.N.Y. 1991)).

⁹⁵ *Id.* at 1005–1006. “System administrators function in cyberspace something like bookstores, something like telephone companies, something like publishers . . . and something like none of these. That makes their rights and obligations difficult to define.” *Id.* at 1054.

be much more significant in cyberspace than it has been to date in real space."⁹⁶ The U.S. Constitution is a local document and cannot be viewed as a blanket standard for online speech given the ease of international communication.

The immense reach of the Internet certainly has the potential to eviscerate or circumvent any traditional jurisdictional and choice of law limitations. It will undoubtedly prompt an increase in forum-shopping, especially where the dispute arises out of areas of law that are substantively different from state to state. The courts may need to re-evaluate their current rules and formulate new solutions to deal with the issues created by the Internet.⁹⁷

This is evidenced by a recent example: A British physicist filed suit against another physicist for a libel allegedly committed on Usenet.⁹⁸ The plaintiff alleged that negative messages had been posted about him from laboratories in Germany and Switzerland, and charged that the messages were read by colleagues and students in Great Britain. He filed the suit in Great Britain, which has particularly harsh libel laws, but, theoretically, could have chosen any forum where the Internet is accessible, giving him the option of picking practically any forum in the world.⁹⁹

Rather than attempt to graft an already-complex body of domestic law onto a dynamic, international medium, other methods of combatting defamatory speech on computer networks are deserving of consideration. First, the ease of access and publication in cyberspace argues strongly for greater value to be placed on the effectiveness of counterspeech. Second, ADR methods of arbitration and mediation could play a more prominent role than they have traditionally played in libel. A vindication-based remedy, grounded in the publication of a finding of falsity by the ADR tribunal, is conducive to the medium of cyberspace. ADR also has the potential to alleviate the jurisdictional problem and would more accurately reflect the developing customs of speech on computer networks.

The ease of access to the Internet and the global publication of many online fora (Usenet, for instance) promises to create a fertile ground for defamation problems in cyberspace. But the same factors also argue for greater emphasis to be placed on the value of counterspeech. If the defamed has at least equal capacity to communicate,¹⁰⁰ by posting to the same Usenet

⁹⁶ *Id.* at 1052.

⁹⁷ Raysman & Brown, *supra* note 93, at 11.

⁹⁸ *See id.*

⁹⁹ *See id.*

¹⁰⁰ There are undoubtedly many situations where this will not be the case. Many areas

newsgroup or BBS where the defamatory utterance appeared, for instance, perhaps this should be encouraged rather than allow reliance on libel litigation:

Litigation isn't the only way to resolve conflicts over free speech on computer networks. America Online general counsel Ellen Kirsch recently lit a small candle of good sense in the gathering cybergloom. A lawyer from a major midwestern firm complained to America Online about postings that, he wrote, "defamed" the product of one of his clients. Kirsch responded by sending the lawyer an AOL starter kit with three hours of free time and urged him to put up his own postings defending the product. Her move was in the tradition of Supreme Court Justice Louis Brandeis, who believed that the solution to "bad speech" was not censorship but more speech.¹⁰¹

Counterspeech will not always satisfy the defamed, of course, and an effective dispute resolution process for online defamation is necessary. ADR potentially could play a much greater role in cyberspace defamation cases than it does in 'real space' defamation cases. Its flexibility and reflection of custom are important considerations in such a novel, easily-accessible international medium.

With such a high potential for jurisdictional and forum-shopping difficulties, a uniform alternative to defamation litigation would be extremely valuable. One form of libel dispute resolution, pioneered by The University of Iowa Libel Research Project,¹⁰² could be a good fit for cyberspace.¹⁰³ This ADR remedy is based not in money damages, but in vindication. A factual hearing is held to determine whether the statement was false and damaging, and the remedy is the publication of the finding of falsity. The publication of a finding of falsity could be particularly effective in cyberspace, where the vindicatory publication could be easily tailored to

in cyberspace are essentially private (private BBSs, for instance). The defamed may not reasonably expect to have an effective power of counterspeech in these instances—his competitive message would not reach those who received the defamatory utterance.

¹⁰¹ Diamond & Bates, *supra* note 6, at 25–26.

¹⁰² See *New Remedy for Libel Claims*, A.B.A. J., Aug. 1987, at 42. See also Pierre N. Leval, *Commentary: The No-Money, No-Fault Libel Suit: Keeping Sullivan in its Proper Place*, 101 HARV. L. REV. 1287, 1300 n.44 (1988).

¹⁰³ The Iowa Project, administered by the American Arbitration Association, is a voluntary alternative to litigation available upon the agreement of both parties. It has not been widely used thus far. See Robert M. Ackerman, *Bringing Coherence to Defamation Law Through Uniform Legislation: The Search for an Elegant Solution*, 72 N.C. L. REV. 291, 300–301 n.48 (1994).

reach those whom the defamatory utterance most likely reached.

Like the use of ADR in other cyberspace dispute contexts, the involvement of specialized third-party neutrals in cyberspace defamation cases would promote an accurate reflection of custom in the dispute resolution process. In an environment with an increasingly well-defined¹⁰⁴ body of custom and where the type of publication, whether it be a permanent web page or a more transitory Usenet posting, is a significant factor in determining the damage done, the necessity of having a neutral well versed in the subject matter is great. A traditional jury simply may not be able to accurately grasp the ramifications of various types of online publication; an effort to effectively educate a jury would be expensive, time-consuming and precarious and would probably add to the already-cumbersome nature of libel litigation. A vindication-based ADR remedy with an expert neutral could be more streamlined, cheaper, quicker and, potentially, a more accurate determination of the parties' interests.¹⁰⁵

III. CURRENT AND FUTURE IMPLEMENTATION OF ADR PROCESSES FOR CYBERSPACE DISPUTES

Systemically, a bottom-up, flexible method of dispute resolution is much more suitable to the dynamic realm of cyberspace than sole reliance on top-down statutory or judicial authority and would not stifle the development of either custom or technology.

There has been speculation that cyberspace eventually could evolve into a separate jurisdiction, with its own rules and adjudicatory authority existing in conjunction with territorial law.¹⁰⁶ The effective resolution of disputes through ADR could be a first step—buying time against a potentially increasing need for more comprehensive blanket legislation and judicial rulemaking.

The rapid and unpredictable growth of technology compels the use, whenever possible, of flexible, bottom-up methods of control:

How do we determine when a "top down" rule such as a statute is best, and when a "bottom up" rule such as private contract . . . is best?

¹⁰⁴ But which may vary widely, depending on the particular electronic "community." See generally HOWARD RHEINGOLD, *THE VIRTUAL COMMUNITY* (1993).

¹⁰⁵ The Iowa Project concluded that libel is especially well-suited to resolution through ADR methods of arbitration and mediation. See Michael Neweity, *Libel Law Then and Now: A Review Essay*, 1989 WIS. L. REV. 359, 400 (reviewing RANDALL P. BEZANSON ET AL., *LIBEL LAW AND THE PRESS: MYTH AND REALITY* (1988)).

¹⁰⁶ See *supra* note 9 and accompanying text (discussing Law Merchant).

The key to answering this question is the recognition that the technology of computer communications is rapidly changing. The number of people using cyberspace, and the number and variety of services being offered on-line, are both growing with astonishing rapidity. In the face of this very dynamic situation, we ought to be reluctant to impose behavior control that is inflexible and uniform beyond the needs of the situation.¹⁰⁷

There is also a sociological reason for a flexible, bottom-up method of control: “[G]iven the proprietary propensities of those who use computer-mediated communication regularly, they would be the most unlikely candidates to relinquish control over their cyberspaces to an outside geopolitical jurisdiction.”¹⁰⁸ Persons who frequently communicate online seem to generally covet some degree of anarchy. They also generally have confidence in their ability to self-regulate,¹⁰⁹ and a top-down implementation of law that conflicts with these customs-in-the-making could face severe opposition from those to whom it is meant to apply. One commentator, paraphrasing the conclusions of an online cyber-law conference, noted:

¹⁰⁷ Hardy, *supra* note 8, at 1025; *see, e.g.*, Eric Schlachter, *Cyberspace, The Free Market and the Free Marketplace of Ideas: Recognizing Legal Differences in Computer Bulletin Board Functions*, 16 HASTINGS COMM. & ENT. L.J. 87, 128 n.233 (1993).

Statutory law written for high-technology issues often has a short shelf life, in that it often includes a detailed account of the technology at that specific time. The federal wiretap statute, updated a few years ago to cover electronic mail privacy, included a detailed description of technology currently used by cordless telephones. “But the new breed of cellular telephones developed almost before ink in the lawbooks was dry . . .” Andrew Petkofsky, *Cyber-Cases Present Challenge: Some Legal Issues Stretching Jurisdiction of Traditional Courts*, RICHMOND TIMES-DISPATCH, Dec. 18, 1994, at A1.

If statutory law with a short shelf life is not recognized as such, it could have a profoundly stifling effect on technological development. *See* John Perry Barlow, *Crime and Puzzlement*, WHOLE EARTH REV. 41, 56 (Fall 1990) (“Today’s heuristical answers of the moment become tomorrow’s permanent institutions of both law and expectation.”).

¹⁰⁸ Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639, 1664 (1995).

¹⁰⁹ *See Id.* at 1656.

Clearly, there was no consensus about what the rules should be in cyberspaces. There was agreement, however, that these budding cybercommunities should be given a chance to develop and test their own rules before the external authorities exert too heavy a hand to bring them into conformity with real-world rules.¹¹⁰

As alluded to throughout this Note, the systemic use of ADR would allow custom to develop, rather than stifle it as a top-down regulatory framework or judicial pronouncement might. A reflection of custom is particularly important in disputes that might focus on what constitutes "reasonable" behavior.¹¹¹ "Most would rather be subjected to the judgments of their virtual community than the local laws of a physical place far from where they live"¹¹²

An intriguing possibility is the use of online "electronic dispute resolution."¹¹³ The use of e-mail technology, as well as real-time chat has the potential to fit very well with the objectives of ADR:

¹¹⁰ Branscomb, *supra* note 108, at 1667 (citing A NEW JURISDICTION FOR CYBERSPACE? A TRANSCRIPT OF NEW JURIS, AN ELECTRONIC CONFERENCE HELD SEPTEMBER-OCTOBER 1993 (I. Trotter Hardy ed., 1994)).

¹¹¹ See Schlachter, *supra* note 107, at 133-134; see also I. Trotter Hardy, *Symposium: Electronic Communications and Legal Change: Electronic Conferences: The Report of an Experiment*, 6 HARV. J. L. & TECH. 213 (1993).

The concept of reasonableness is pervasive in Anglo-American law, especially tort law. There is no inherent reason why the concept cannot apply in cyberspace. The problem is that in many situations, jurors—and even cyberspace users themselves—may not know and may have no basis for knowing what is reasonable in cyberspace.

Hardy, *supra* note 8, at 1013.

¹¹² Petkofsky, *supra* note 107, at A1 (paraphrasing Professor Hardy).

¹¹³ The discussion here will focus on using cyberspace to solve cyberspace-related disputes. For an argument that online "EDR" could also be used effectively to resolve minor, non-cyberspace disputes, see Perritt, *supra* note 22, at 1012.

The process will allow for greater flexibility, more creative solutions and quicker decisions. More important, the impersonality will preserve the relationship between the parties once the dispute is resolved. This will bring to the forefront alternative dispute resolution options such as . . . mediation, arbitration and mini-trials. All these dispute resolution alternatives are more conducive to the electronic medium than is the courtroom, especially when there is a lack of trust between the parties, and emotions stand in the way of effective communication. Even when there is a serious economic imbalance between the parties, access to the highway to resolve the dispute makes sense: The economic size of the parties is "invisible" to the particular dispute resolution process.¹¹⁴

Online ADR is already being explored. At the forefront is the Virtual Magistrate project,¹¹⁵ directed by Robert Gellman and a joint venture of the Cyberspace Law Institute, the American Arbitration Association (AAA), the Villanova Center for Information Law and Policy and several online service providers and public interest groups.¹¹⁶ The project is funded by the National Center for Automated Information Research (NCAIR), a New York-based law and technology research foundation.¹¹⁷

Virtual Magistrates are available to resolve disputes catching service providers between conflicting claims over copyright, misuse of network communications channels or libel or slander. Such disputes can be submitted through a World Wide Web page maintained at Villanova, assigned to a magistrate by the AAA administrator, and resolved within 72 hours. Complaints, answers, hearings and awards all are electronic, exchanged through specialized Web pages and dockets maintained on the World Wide Web. In the first case resolved by a virtual magistrate, America Online was ordered to remove an advertisement offering to provide mailing lists of thousands of email addresses.¹¹⁸

¹¹⁴ Ronald J. Postums, *The Trillion Dollar Risk*; BEST'S REV.—CASUALTY INS. EDITION, Sept. 1994, at 36, 110. See, e.g., Perritt, *supra* note 22, at 1012. "[E]very good mediator knows that reducing emotion can aid dispute resolution communication." *Id.*

¹¹⁵ The Virtual Magistrate, <http://vmag.law.vill.edu:8080/>. Another recent effort aimed at facilitating the resolution of disputes arising from online activity is the Online Ombuds Office, <http://www.ombuds.org/>.

¹¹⁶ See Press Release: Conference on Online Dispute Resolution, <http://vmag.law.vill.edu:8080/docs/press/press.960529.html/>.

¹¹⁷ See *id.*

¹¹⁸ *Id.*

The resolution of online-oriented disputes online would eliminate fairness issues related to the expense of travel. Such issues are particularly important considering that disputes will increasingly raise international choice-of-law and jurisdictional questions. The ability to present the case and obtain a decision within three days, as the Virtual Magistrate project is designed to facilitate, is also a major selling point. The Virtual Magistrate is the prototypical online dispute resolution facility; while it has not been widely used thus far, awareness of the need for a specialized cyberspace dispute resolution mechanism has been growing.¹¹⁹

Online ADR might appeal strongly to less sophisticated, individual parties with cyberspace grievances. While relatively simple disputes would probably be served very well by e-mail and chat-based communication,¹²⁰ online ADR's ability to effectively resolve more complex disputes will likely increase as technology increases. Development will not stop with e-mail and real-time chat; more "experiential" media such as two-way video and audio are developing rapidly.¹²¹

Traditional applications of ADR, in the commercial or intellectual property contexts, for instance, typically rely to various degrees on the underlying body of law. A cyberspace-oriented ADR institution could lie somewhere between a pure adjudicatory model, with little reliance on pre-existing rules, and a simple forum for the rule enforcement of a chosen legal system, incorporating expert neutrals to make determinations dependent on the unique nature of cyberspace ("reasonableness" determinations, for example).

Although rulemaking and adjudication are conceptually distinct modes of decisionmaking they can be combined in practice. An adjudicator may make new rules just as a traditional common law court makes new rules to fit cases of first impression. It is possible to have a system in which there is only adjudication. A claimant need not make a claim of right in the sense that the claimant identifies some pre-existing rule under which his case falls. In such a system the adjudicator would have very broad discretion to decide whether a particular transaction is "fair." For example, a dispute arises over acceptable use of internetworking facilities, and a committee of members of the Internet

¹¹⁹ On May 22, 1996, a group of fifty experts in law, technology and information services concluded a one day meeting in Washington to evaluate the prospects for such specialized cyberspace "courts." The conference was administered by the NCAIR. *See id.*

¹²⁰ *See* Perritt, *supra* note 22, at 1013.

¹²¹ *See* Hardy, *supra* note 8, at 1053.

meet to decide how the dispute should be resolved fairly, without reference to any pre-existing rules, because there are none. [sic]¹²²

Enforceability of the ADR arbitral decrees and of contracts to arbitrate should not be a problematic issue. First, judicial recognition of and enforcement of ADR decisions has increased.¹²³ Assuming the procedure is facially fair, there should be few major problems with judicial aid in enforcing ADR decisions. And, as contract law will play a very large role in the development of cyberspace jurisprudence, a dispute resolution system which has its underpinnings in contract doctrine is particularly suitable:

Modern contract law retains the flexibility and malleability of traditional contract theory. Since contract law enables the parties to forge unique solutions to emergent legal problems, it is particularly well suited for the new information technologies. Contract law's capacity to evolve as a voluntary social institution is in contrast with the coercive features of tort law. *General contract law principles fit well with the emergent culture of the Internet, which eschews involuntary obligations, whether imposed from the state or from tort law.*¹²⁴

The second major tool of enforceability could be a threat in the form of "cooperative exile" and would rely heavily on a "private association" model. This, too, is grounded in contract.¹²⁵ An association of networks, or

¹²² Henry H. Perritt, Jr., *Dispute Resolution in Electronic Network Communities*, 38 VILL. L. REV. 349, 389 (1993).

[T]he failure of the decisionmaker to give reasons or to make findings of fact and conclusions of law, and the absence of a formal record do not impair the legal quality of the ultimate decision. On the other hand, if the procedure gets too far away from an adversarial presentation of material facts and does not provide an opportunity to make legal arguments, the essential characteristics of adjudication may not be present and the finality of the award may be questionable under the *RESTATEMENT (SECOND) OF JUDGMENTS* as well as the status of the process as arbitration under the Arbitration Acts.

Id. at 393.

¹²³ See Dick, *supra* note 29, at 52-53.

¹²⁴ Rustad & Eisenschmidt, *supra* note 10, at 263 (emphasis added).

¹²⁵ It is not a new idea that people who make up a community can get together and contract among themselves to make rules that apply to themselves. That is what corporations do and that is what private associations like churches, fraternities, and other nonprofit organizations do. That is the way employment relationships and employee benefit plans work, both with or without unions. Such private associations also have the legal power to design and use specialized adjudicatory institutions. That is

networks and system administrators, or system administrators and users, or simply system administrators, could contractually establish the validity of the ADR institution and its decisions.¹²⁶ If a party fails to adhere to an ADR decree, he or she potentially could be "exiled" through the cooperative action of those in the association.¹²⁷ Such a notion would require an extraordinary degree of cooperation, but it might be eased by some sort of technological improvement if the need for an ultimate source of enforcement is perceived to be great enough. If there is not enough cooperation to establish a sort of private association, this may be an appropriate area for a governmental authority to give its stamp of approval and support in enforcement.

ADR could play a very large role in the resolution of many disputes involving recent information technologies. There are many practical reasons in favor of choosing ADR over litigation. Its self-regulatory nature would promote, rather than stifle, the natural evolution of a coherent body of cyberspace customary law. And as a continuation of its recent growth, ADR would alleviate some legal-application problems relating to the rapid development of both technology and a global economy.

called arbitration.

Perritt, *supra* note 22, at 1008 n.50.

¹²⁶ See Perritt, *supra* note 122, at 361.

¹²⁷ See *id.*; see also *id.* at 356-357 (discussing disconnection model of rule-enforcement generally, and transaction costs associated with changing service providers).