## University of Florida Journal of Law & Public Policy

Volume 3 | Issue 1 Article 5

1990

# Impending Legal Issues for Integrated Broadband Networks

Michael I. Meyerson

Follow this and additional works at: https://scholarship.law.ufl.edu/jlpp

#### **Recommended Citation**

Meyerson, Michael I. (1990) "Impending Legal Issues for Integrated Broadband Networks," *University of Florida Journal of Law & Public Policy*: Vol. 3: Iss. 1, Article 5.

Available at: https://scholarship.law.ufl.edu/jlpp/vol3/iss1/5

This Article is brought to you for free and open access by UF Law Scholarship Repository. It has been accepted for inclusion in University of Florida Journal of Law & Public Policy by an authorized editor of UF Law Scholarship Repository. For more information, please contact kaleita@law.ufl.edu.

# IMPENDING LEGAL ISSUES FOR INTEGRATED BROADBAND NETWORKS

### Michael I. Meyerson\*

I.	Introduction	49
II.	HACKING AND VIRUSES	50
III.	Privacy	51
IV.	PORNOGRAPHY	55
V.	REFUSAL TO DEAL	60
VI.	Whose Speech Is It?	62
VII.	Conclusion	63

#### I. Introduction

The future of integrated broadband networks (IBNs)¹ has yet to arrive. Although the extraordinary theoretical technical capacities of this new form of transmission seem well established, the ultimate use for IBNs is not. That must await the answer to many questions: Which entities will operate IBNs? Which businesses will choose the use IBNs? Which services will offer IBNs? What will be the long-term regulatory environment for IBNs? Perhaps most importantly, which IBN services will consumers want? Due to these unanswered questions, many aspects of the future of IBNs remain unclear.

Given human nature, however, specific legal problems are certain to arise. The insatiable human appetite for mischief, information, pornography, and anti-competitive activity guarantees that the many legal conflicts that afflict computers, telephones, cable television, and broadcasting will be visited upon IBNs. This article focuses on several of these legal problems. By examining the history of recent controversies involving the electronic media and breaches of security, protection of

<sup>\*</sup> Assistant Professor of Law, University of Baltimore School of Law. B.A., 1976, Hampshire College; J.D., 1979, University of Pennsylvania Law School.

<sup>1.</sup> An integrated broadband network on fiberoptic cable (IBN) is a new technology which is capable of carrying an abundance of information formerly delivered via broadcast, telephone wires, and print. IBNs transmit voice, image, video, and data over a single digital fiberoptic circuit. This technology can provide a full range of services, from carrying the public telephone net to cable television, as well as several new services such as picture telephony, high-speed videotex and video-conferencing.

privacy, regulation of sexual material and refusals to deal and similarities or differences between the "old" technologies and IBNs, this article attempts to outline some possible solutions to forestall, or limit, future legal conflicts<sup>2</sup> in the use of IBNs.

#### II. HACKING AND VIRUSES

The 1980s revealed the fragility of computer security. In 1983, a group of teenagers used a simple home computer to break into the radiation treatment computer at the Memorial Sloan Kettering Cancer Center, gaining not only access to the treatment records of patients, but also the ability to alter the radiation level each patient received.<sup>3</sup> A "logic bomb" sabotaged the central computer at the Los Angeles Department of Water and Power in 1985, rearranging data and making critical information temporarily inaccessible.<sup>4</sup> And in 1988, a computer virus, allegedly created by a twenty-three year old graduate student, quickly paralyzed 6,000 military and university computers across the country.<sup>5</sup>

The two-way capabilities of an IBN create similar possibilities for mischief. One promised benefit of an IBN is that individuals can transmit as well as receive information. Once people hook into the network, however, preventing the next generation of hackers from either breaking into the information stream of others or sending destructive impulses into the system will be difficult.

Current law is unable to cope with the recent assaults on computer systems, and thus is unlikely to prevent and punish invasions of IBNs. For example, the Federal Computer Fraud and Abuse Act of 1986 makes it a crime to "intentionally, without authorization, access any computer of a department or agency of the United States." Since the verb "access" is not defined, the question of whether a person who creates a computer virus which jumps from one program to another violates the Act remains unanswered. Further, "intent" is difficult to establish where a case involves a simple prank.

<sup>2.</sup> There is one critical preliminary issue that must be resolved: the regulatory status of IBNs. Numerous legal questions depend on whether IBNs are classified as common carriers. These questions include who is permitted to own IBNs and whether there is governmental regulation of rates and business practices of IBNs. These issues have been well-analyzed in Botein, The Regulatory Status of Integrated Broadband Networks: A Preliminary Inquiry, 3 U. Fla. J.L. & Pub. Pol'y 65 (1990).

<sup>3.</sup> Yee, Juvenile Computer Crime, 7 COMM. ENT. 335 (1984).

<sup>4.</sup> Stewart, Police Plug Into Computer Criminal, L.A. Times, June 2, 1985, at 2.

<sup>5.</sup> Branscomb, Rogue Computer Programs and Computer Rogues, 16 RUTGERS COMPUTER & TECHNICAL L.J. 1, 6-11 (1990).

<sup>6. 18</sup> U.S.C. § 1030(a)(3) (Supp. 1990).

Similarly, federal wiretap laws may fail to prevent invasions. The Omnibus Crime Control and Safe Streets Act of 1968<sup>7</sup> was amended in 1988 to prohibit the interception of wire or oral electronic communications.<sup>8</sup> The focus of the Act, however, is on protecting "communication," the passing of information between parties, rather than on protecting all information, including that which has been generated but not communicated to others.<sup>9</sup> The Act also contains no restrictions on those who might add to or alter information in a system.

Since destruction of information transmitted by an IBN would have a devastating effect, not only on the users of the system, but on the future development of IBNs generally, criminal penalties for destroying IBN transmitted information should be enacted before IBNs become totally operational. The law must protect both the IBN and the information that the IBN transmits. The law should make it a felony:

- A) to knowingly insert information or instructions into an IBN which does or is likely to alter, delay, disrupt or destroy any other information or programming transmitted either over the IBN or through a device connected to the network;
- B) to knowingly obtain information or programming without authorization through an IBN;
- C) to use an IBN to obtain money, property or services by false or fraudulent means:
- D) to copy information or proprietary programs without the permission of the owner; or
- E) to knowingly use or disclose codes, passwords, and similar means of access to information without the consent of the owner.

Penalties for violating the law should be severe, including punishment by fine and imprisonment. Additionally, any individual or entity that suffers a loss due to a violation of the law should have a civil damage claim against the violators.

#### III. PRIVACY

IBNs will be able to offer consumers and businesses a wide range of services. A single IBN system can provide all of the following: high definition television, non-broadcast video entertainment, picture telephones, home shopping, home security, polling, data bases and vid-

<sup>7. 18</sup> U.S.C. §§ 2510-2540 (Supp. 1990).

<sup>8. 18</sup> U.S.C. § 2511(1)(a) (Supp. 1990).

<sup>9. 18</sup> U.S.C. § 2510(1), (2) (1988).

eotext. However, this extensive capability also means that an enormous amount of personal information will flow through the same conduit. The ease and low cost of compiling this private data will pose a direct threat to consumer privacy and business proprietary information.

Historically, when information is compiled, others seek access to it. For example, government agents can peruse library records to see which books an individual reads. 10 Additionally, in Utah, when one supplier of telephone services was charged with violating laws on telephone pornography, the United States Attorney attempted to subpoena records to identify which individuals had voluntarily called the service. 11 Similarly, the owner of an Ohio adult movie theater charged with exhibiting obscene movies sought a court order to obtain the names of the cable subscribers who viewed similar movies on the local cable television system. 12 Further, the direct mail market industry continually seeks improved, more precise information about the American public. The wealth of information potentially conveyed over an IBN would be economically attractive to those seeking to locate potential customers. Finally, creditors, insurers and employers may also have a similar economic use for the information carried by an IBN.

If violations of either individual or business privacy occur when IBNs initially become available, however, the resulting lack of consumer trust in IBNs could hinder or doom their development. Accordingly, by the time IBNs finally become operational, privacy protection should already be in place. Existing legislation, especially the Federal Cable Act<sup>13</sup> and Fair Credit Reporting Act,<sup>14</sup> provide a useful framework for IBN protection.

The Cable Act wisely draws a distinction between "personally identifiable information," which can identify particular persons or households, and "aggregate data" which only analyzes large groups but does not permit individual identification. <sup>15</sup> All limits in the Act on gathering and distributing information for cable television refer only to "personally identifiable information." <sup>16</sup> The same rule should apply to IBNs.

<sup>10.</sup> See Brown v. Johnston, 328 N.W.2d 510 (Iowa), cert. denied, 463 U.S. 1208 (1983).

<sup>11.</sup> See Carlin Communications, Inc. v. FCC, 837 F.2d, 546, 557 n.4 (2d Cir. 1988).

<sup>12.</sup> See D. Nash & J. Smith, Interactive Home Media and Privacy 52-57 (1981). The cable company ultimately agreed to provide only aggregate viewing data that did not disclose individual names. *Id.* at 53.

<sup>13. 47</sup> U.S.C. §§ 521-559 (Supp. 1990).

<sup>14. 15</sup> U.S.C. § 1681 (Supp. 1990).

<sup>15. 47</sup> U.S.C. § 551(a)(2) (Supp. 1990).

<sup>16. 47</sup> U.S.C. § 555(b) (Supp. 1990).

Similarly, two exceptions in the Cable Act are applicable to IBNs. First, a cable operator may collect personal information that is necessary for providing a service to the subscribers.<sup>17</sup> Obviously, a cable operator offering pay-per-view must know what program the paying customer wants to receive. Such information is essential for the IBN operator as well. Second, the cable operator can sweep the system to search for unauthorized reception of cable service.<sup>18</sup> Again, the IBN operator should also be able to insure that only those paying for a service are receiving it.

A related issue concerns how the collection and dissemination of personal information should be authorized. The Cable Act requires "positive consent" by the subscriber's affirmative act rather than permitting the cable operator to imply consent from a subscriber's failure to respond to a request for permission. <sup>19</sup> Requiring positive consent is crucial, since it provides the only means for insuring that the subscribers knowingly and voluntarily consented.

An additional limitation needed on the collection of information is the disposal of personally identifiable information after a specified period of time. The Cable Act requires cable operators to destroy information when no need remains for the purposes for which it was acquired.<sup>20</sup> Alternatively, the Fair Credit Reporting Act prescribes specific time limits after which "obsolete" information must be destroyed.<sup>21</sup> These time controls help limit the potential damage arising from any future breach of security.

The limitations on the dissemination of information compiled through an IBN should be similar to the limits outlined above for the collection of information. Unless specific consent has been given, information should only be disclosed under certain conditions. First, a private entity should only receive information that is necessary for the provision of a specifically requested service. Thus, the transfer of information by either a provider of an IBN service, an IBN operator, or a parent or related company would *not* be necessary for the provi-

<sup>17. 47</sup> U.S.C. § 551(b)(2)(A) (Supp. 1990).

<sup>18. 47</sup> U.S.C. § 551(b)(2)(B) (Supp. 1990).

<sup>19.</sup> H.R. REP. No. 934, 98th Cong., 2d Sess. 77 (1984). (This legislative history to the Cable Act is generally termed "House Report.") The only exception to the requirement for "positive consent" is for the distribution of subscribers' names and addresses for mailing list purposes. The information that may be given out pursuant to this exception is quite limited; no private data, such as the choice of programming viewed or transactions made of the system, may be conveyed. 47 U.S.C. § 551 (c)(2)(c) (Supp. 1987).

<sup>20. 47</sup> U.S.C. § 551(e) (Supp. 1990).

<sup>21. 15</sup> U.S.C. § 1681(c) (1988).

sion of a requested service and should be prohibited. This rule has the additional benefit of limiting the competitive advantage a monopoly IBN operator might have if permitted to compete in the provision of non-monopoly services.

Governmental entities might also seek information compiled through an IBN. The 1977 Report of the Privacy Protection Study Commission recommends that personal information, "should not be accessible to government unless government can show a compelling interest that outweighs the individual's interest to be free from government intrusion."<sup>22</sup> Similarly, the Cable Act requires that a government entity prove by clear and convincing evidence that the subject of the information sought is a reasonable suspect of criminal activity and that the information sought would be material evidence.<sup>23</sup> Thus, in a situation similar to that of the Ohio adult movie theater owner, the Cable Act would prohibit the disclosure of the names of cable subscribers because the suspect of criminal activity was the adult movie owner, not the subscribers.

The Cable Act also requires that the subject of the information receive notification of the request for information and have the opportunity to contest the government's request. This additional requirement insures that the subject of the information will know when information is requested and that the safeguards are followed. Further, to make the legal protections meaningful, consumers must be fully informed of their rights. Thus, IBN operators should be required to give periodic notice of consumer rights to the consumers using the network. A mechanism that permits individuals to learn what information an IBN maintains on them and allows individuals to correct erroneous information in their files is also needed. The Fair Credit Reporting Act requires credit agencies to review disputed information and either correct the information or permit consumers to send recipients of the disputed information the consumer's opposing or explanatory statement.

Heavy penalties should be imposed on violators of the privacy rules. IBN operators, service providers, and their employees should

<sup>22.</sup> Privacy Protection Study Commission, Personal Privacy in an Information Society 362 (1977).

<sup>23. 47</sup> U.S.C. § 551(h) (Supp. 1990).

<sup>24. 47</sup> U.S.C. § 551(c)(2), 551(h) (Supp. 1990); House Report, at 77-79.

<sup>25.</sup> This is similar to the Cable Act's requirement that cable operators give annual notice of privacy rights to subscribers. 47 U.S.C. § 551(a) (Supp. 1990).

<sup>26. 15</sup> U.S.C. § 1681(i) (1990). The Cable Act requires that subscribers be given a "reasonable opportunity to correct any error in information," 47 U.S.C. § 551(d) (Supp. 1990), but does not detail the procedures that are involved.

all be subject to civil and criminal penalties. The individual whose privacy has been violated should recover compensation for damages suffered, with at least a statutory minimum recovery plus attorney fees. Additionally, the government should criminally prosecute offenders to enforce privacy protection. Ultimately, specific legal responsibility for creating a system capable of safeguarding information must be assigned.<sup>27</sup> IBN operators and service providers should both be a part of this system. As technology advances, responsibility for protection should expand to include all reasonable physical and electronic safeguards of personally identifiable information.

## IV. PORNOGRAPHY

Apparently, those wishing to disseminate pornographic material operate in all effective mediums. For every form of communication, some choose to convey what others would term pornography. Inevitably, IBNs will transmit pornography. The question is, how will society choose to react?

Pornography is not a legal term, but merely common parlance for depictions of sexual activity that some consider offensive. The legal term "obscenity" describes material falling beyond the protection of the first amendment.<sup>28</sup> Without the protective shield of the first amendment, the use of obscene material can be severely limited. Consequently, questions arise, because the test for "obscenity," is difficult to evaluate. For material to be classified legally obscene, the Supreme Court asks:

(a) whether the average person, applying contemporary community standards, would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political or scientific value.<sup>29</sup>

However, the Supreme Court treats children differently than adults in the determination of obscenity. Acceptable material for adults may still be obscene for children if the work appeals to the prurient interests of children, is patently offensive to children, and lacks serious value

<sup>27.</sup> Such a requirement is noticeably absent from the Cable Act.

<sup>28.</sup> Roth v. United States, 354 U.S. 476, 485 (1957).

<sup>29.</sup> Miller v. California, 413 U.S. 15, 24 (1973). Legal obscenity is frequently referred to as "Miller obscene." *Id.* at 24.

for children.<sup>30</sup> Thus, society can protect minors from material that is inappropriate for minors, even if the material is otherwise protected by the first amendment. The government may not, however, "reduce the adult population to reading only what is fit for children."<sup>31</sup> This dichotomy creates a twisted path of cases, resulting in a variety of standards for permissible regulation that change with the medium.<sup>32</sup>

For broadcasting, the Supreme Court permits the Federal Communication Commission (FCC) to ban, at least during the middle of the day, programming that is "indecent" but does not rise to the level of obscenity.<sup>33</sup> The current definition of "indecency" is "language or material that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards for the broadcast medium, sexual or excretory activities and organs."<sup>34</sup> Thus, "dirty words" and "dirty pictures" can be kept from the airwaves, even without a showing that they appeal to prurient interest and even if the program, as a whole, presents material of serious value.<sup>35</sup>

The Supreme Court permits the banning of indecent broadcasting because that broadcasting is "uniquely pervasive" and "uniquely accessible to children."<sup>36</sup> The Court notes that, unlike book sellers and movies theater owners, broadcasters can not segregate the children in their audience from adults.<sup>37</sup> Since broadcast programs are easily obtained by unsupervised children, indecent material can be withheld from children only by stopping the source of the programming.

The situation differs for cable television. As with other media, cable is prohibited from disseminating obscene material.<sup>38</sup> Unlike

<sup>30.</sup> Ginsberg v. New York, 390 U.S. 629 (1968).

<sup>31.</sup> Bolger v. Young's Drug Prod. Corp., 463 U.S. 60 (1983) (quoting Butler v. Michigan, 352 U.S. 380, 383 (1957)).

<sup>32.</sup> See infra notes 33-57 and accompanying text.

<sup>33.</sup> FCC v. Pacifica Found., 438 U.S. 726 (1978).

<sup>34.</sup> In Re Infinity Broadcasting, 3 FCC Reg. 930 (1988). The original definition of indecency also included the limitation that a determination of offensiveness must consider whether a broadcast occurred "at times of the day when there is a reasonable risk that children may be in the audience." Pacifica, 438 U.S. at 732 (quoting FCC regulations, 56 FCC 2d 94, 98 (1975)). Under current federal law, indecent broadcasts are banned 24 hours a day. 18 U.S.C. § 1464. This total ban, however, may be suspect since it fails to consider whether the need to protect children outweighs the interests of adults from obtaining the material. See Action for Children's Television v. FCC, 852 F.2d 1332 (D.C. Cir. 1988).

<sup>35.</sup> Pacifica, 438 U.S., at 750-51.

<sup>36.</sup> Id. at 748, 749.

<sup>37.</sup> Id. at 749.

<sup>38.</sup> It is a federal criminal offense to transmit obscene cable programming, punishable by a fine or imprisonment for up to two years or both. 18 U.S.C. § 1468 (1988).

broadcasting, however, courts have consistently refused to prevent localities from banning indecent programming from cable television.<sup>39</sup> Cable differs from broadcasting because its technology permits each individual homeowner to decide whether specific channels should enter the home. Both addressable converters and so-called "lock-boxes" permit individuals to block out programming they find offensive.<sup>40</sup> Thus, children can be protected without silencing the source.

Telephones have created many legal battles. In 1983, federal law criminalized "dial-a-porn." After repeated litigation and three sets of FCC regulations, the law, at least in some form, passed judicial scrutiny. The first FCC regulation permitted dial-a-porn only during 9:00 p.m. and 8:00 a.m. eastern standard time or to those paying by credit card. This regulation, however, made dial-a-porn available from 6:00 p.m. to 5:00 a.m. in California, but presumably children on the West Coast have different bed times. The Court of Appeals for the Second Circuit found this regulation unconstitutional because it unnecessarily restricted the ability of adults to use dial-a-porn services. Two years later, the same court struck down the second set of FCC regulations that replaced the time-channeling restriction with a requirement that providers of dial-a-porn send messages only to adults who had obtained a special identification code. The court ruled again

<sup>39.</sup> Wilkinson v. Jones, 107 S. Ct. 1559 (1987), affg mem. 800 F.2d 989 (10th Cir. 1986), affg Community Television, Inc. v. Wilkinson, 611 F. Supp. 1099 (D. Utah 1985); Cruz v. Ferre, 755 F.2d 1415 (11th Cir. 1985); Community Television, Inc. v. Roy City, 555 F. Supp. 1164 (D. Utah 1982); Home Box Office, Inc. v. Wilkinson, 531 F. Supp. 987 (D. Utah 1982). Although the Supreme Court affirmed a decision striking down a cable indecency law, the Court did not issue an opinion, thus it is not certain whether all cable indecency laws are invalid. See Meyerson, The Right to Speak, The Right to Hear, and the Right Not to Hear: The Technological Resolution to the Cable/Pornography Debate, 21 MICH. J. LAW REF. 137, 156-57 (1987).

<sup>40.</sup> The Cable Act requires cable operators to make such devices available to all subscribers who request them. 47 U.S.C. § 554(d)(2)(a) (Supp. 1987).

<sup>41. 47</sup> U.S.C. § 223(b) (Supp. 1987). That is the use of a telephone for making, "any obscene or indecent communication for commercial purposes to any person under eighteen years of age . . . ." Id.

<sup>42.</sup> FCC regulations promulgated in the Third Report and Order, Enforcement of Prohibitions Against the Use of Common Carriers for the Transmission of Obscene Materials, 2 FCC Reg. 2714 (1987) were finally upheld in Carlin Communications, Inc. v. FCC, 837 F.2d 546 (2d Cir. 1988) ("Carlin III"), after previous rules were struck down in Carlin Communications, Inc. v. FCC, 749 F.2d 113 (2d Cir. 1984) ("Carlin I") and Carlin Communications, Inc. v. FCC, 787 F.2d 846 (2d Cir. 1986) ("Carlin II").

<sup>43.</sup> See Carlin I, 749 F.2d at 113 (quoting Report and Order, 49 Fed. Reg. 24996, 25003 (1989).

<sup>44.</sup> Carlin I, 749 F.2d at 123.

<sup>45.</sup> Carlin II, 787 F.2d at 856.

that less restrictive means such as blocking devices, existed for protecting children.

Ultimately, the court of appeals upheld the FCC's third set of regulations that provided dial-a-porn could be transmitted if the service required credit card payment prior to transmission, an identification code obtainable by written application, or scrambled messages making the service only obtainable through a descrambling device. <sup>46</sup> The court ruled that these requirements reached a proper balance by restricting the ability of children to receive the service, while imposing non-burdensome restrictions on service providers and willing adult customers. <sup>47</sup> The court, however, found the provision governing indecent programming unconstitutional. <sup>48</sup> Finding that technology exists to protect individual homeowners and that callers must affirmatively seek the phone messages, current law prohibits the regulation of indecent phone messages. <sup>49</sup> Thus, the court ruled that only obscene messages are prohibited. <sup>50</sup>

Once a court determines that the service is obscene, the FCC does not need to search for "the least restrictive alternative." The government's interest in protecting adults' right to receive information that is obscene for children, was premised on adults' constitutional right to receive communication protected by the first amendment. Since obscenity is *not* protected by the first amendment, constitutionally the right of adults to receive obscene telephone messages is not of particular concern to the FCC. Such solicitude is only warranted for protected speech, which includes indecent speech. The court of appeals, however, seemed to confuse the obscenity/indecency dichotomy with the concept that services can be obscene for minors, but not for adults. For the latter situation, consideration for the rights of adults to receive the indecent programming is indeed appropriate, since indecent programming is protected communication for adults.

In response to the trio of cases addressing minors' access to dialaporn, Congress amended the law in April 1988 to prohibit obscene

<sup>46.</sup> Third Report and Order, 2 FCC Reg. 2714, 2719-20 (1987).

<sup>47.</sup> Carlin III, 837 F.2d at 556. The Court added that the FCC would have to reconsider its ruling were a simpler protective device to become available. Specifically, the Court referred to a system whereby the service provider would precede its message with a three-tone sound. An inexpensive listening device, installed at home telephones, would immediately disconnect the telephone line from all desiring to block the services. The Court found that if this device were technically feasible, it might be the least restrictive means for regulating dial-a-porn. Id.

<sup>48.</sup> Carlin III, 837 F.2d at 560.

<sup>49.</sup> Id.

<sup>50.</sup> Id.

<sup>51.</sup> Ginsberg, 390 U.S. at 639-40.

and indecent commercial telephone communication to any recipient. regardless of age. 52 The Supreme Court upheld the ban on commercial telephone obscenity, but found the prohibition on indecent commercial telephone communication unconstitutional. 53 The Court held that the earlier FCC rules showed a "feasible and effective" method existed for protecting children from indecency.<sup>54</sup> The Court also noted that the danger for a "surprised" listener was not the same with telephone as with broadcasting, because the recipients of telephone messages are callers, who voluntarily seek the messages. 55 The Court also accepted the fact that some children would be able to circumvent any technological safeguard by stating that "a few of the most enterprising and disobedient young people will manage to secure access to such messages."56 Because this number was relatively small, the Court concluded that the total ban on indecency was "not a narrowly tailored effort to serve the compelling interest of preventing minors from being exposed to indecent telephone messages."57 How does this affect IBNs? Certainly under current law, obscene programming and services can be banned, from the network. The unsettled areas concern whether indecent, but not obscene, programming and services can be banned and how to protect children from material that is obscene for them, but not obscene for adults.

The technology of IBNs will probably permit individual homeowners to decide what programming and services enter their homes. Scrambling and locking devices will enable only those who wish to receive certain programming to do so. As with telephones and cable television, IBNs should rely on individual, rather than governmental, censorship to control indecent communication.

Scrambling and locking devices will also permit parents to protect their children from receiving programming that is obscene for minors. As with telephones, any regulation of such material should involve the least restrictive alternative for adults' right to receive constitutionally protected communication. Thus, a requirement that any IBN

<sup>52. 47</sup> U.S.C. § 223(b), amended by Pub. L. No. 100-297, 102 Stat. 424 (1988). The law also removed the FCC's rules, on the theory that special protections were not needed since a total ban was in effect. Later in 1988, this law was further amended to permit enforcement of the dial-a-porn ban, but only through criminal prosecutions. Pub. L. No. 100-690, 102 Stat. 4502 (1988).

<sup>53.</sup> Sable Communication of Cal., Inc. v. FCC, 109 S. Ct. 2829 (1989).

<sup>54.</sup> Id. at 2837.

<sup>55.</sup> Id.

<sup>56.</sup> Id. at 2838.

<sup>57.</sup> Id. at 2839.

which services providers and programmers of "obscene for children" communications assist parents with restricting the communication may be permissible. Possible alternatives include prior notification of such programming or services and grouping such programs together, making blocking devices effective. Once parents are empowered to protect their children, other adults who desire the "obscene for children" communication should receive it.

One question of censorship remains. Should the operator of the IBN be permitted to censor? The telephone cases show a discomforting trend. Michigan Bell, for example, decided to exclude a host of services that the company found, "inflammatory, and likely to offend ethnic, gender, racial or religious groups; lewd, lascivious, indecent or obscene; . . . or likely to have a detrimental effect on Michigan Bell's image or reputation." The danger of private censorship, unchecked by either competitive pressure or constitutional requirements, is undesirable.

One court, in upholding telephone company censorship, found that because the service went to many listeners simultaneously, "the phone company resembles less a common carrier than it does a small radio station." Accordingly, the court allowed the telephone company to edit the service. The court erred in its reasoning, however, since the service provider, not the telephone company, is broadcasting; the service provider should be the one compared to a radio station, not the telephone company. The telephone company merely acts as the conduit through which the messages are transmitted. The role of conduit and content should not be confused. Laws permitting protection not only of minors but the "image and reputation" of a company, permit the unilateral and unlimited power to censor.

#### V. REFUSAL TO DEAL

The history of electronic communications is replete with conflicts of vertically integrated monopolies refusing to deal with potential competitors. In these conflicts, much depends on who receives the governmental right to control access to essential facilities. In the 1980s, providers of long distance telephone service litigated to gain the right

<sup>58.</sup> Quoted in Pepper, Through the Looking Glass: Integrated Broadband Networks, Regulatory Policies, and Institutional Change 66 (OPP Working Paper Series No. 24; Office of Plans and Policy, FCC, November 1988) (emphasis added).

<sup>59.</sup> Carlin Communications, Inc. v. Mountain States Tel. & Tel. Co., 827 F.2d 1291, 1294 (9th Cir. 1987).

<sup>60.</sup> Id. 827 F.2d at 1297.

to connect to local telephone exchanges.<sup>61</sup> Cable television operators were also struggling to gain access to telephone poles for their cable network. In response, some telephone companies, often desiring to construct the cable facilities themselves, denied access altogether or charged exorbitant monopoly prices to the cable television operators.<sup>62</sup>

Similarly, cable operators act anti-competitively by using their exclusive franchising to help their own programming services. For example, cable companies who own pay movie channels may remove or bar competing programmers from their systems. <sup>63</sup> Additionally, cable-owned popular programming services have been denied to cable's competitors, such as multichannel, multipoint distribution systems. <sup>64</sup> Overall, those in control of essential facilities tend to benefit their own vertically-integrated corporate siblings.

Consequently, policy makers and regulators need to design a regulatory system which prohibits anti-competitive behavior regardless of the eventual industry structure. The decision as to which regulatory structure is chosen for IBNs should reflect this consideration. Further, once a structure is chosen, procompetitive safeguards must be implemented.

Initially, the physical architecture of the IBN must be one that encourages multiple users. One possible model is the Open Network Architecture (ONA) which the FCC requires the Bell Operating Com-

<sup>61.</sup> MCI Communications Corp. v. American Tel. & Tel., 708 F.2d 1081 (7th Cir.), cert. denied, 464 U.S. 891 (1983).

<sup>62.</sup> See, e.g., TV Signal Co. v. American Tel. & Tel., 617 F.2d 1302 (8th Cir. 1980). The Federal Pole Attachment Act permits the regulation of the rate a utility charges a cable operator for use of the pole. 47 U.S.C. § 224 (Supp. 1987).

<sup>63.</sup> See, e.g., New York Citizens Comm. on Cable TV v. Manhattan Cable TV, Inc., 651 F. Supp. 802 (S.D.N.Y. 1986). See also Nadel, COMCAR: A Marketplace Cable Television Franchise Structure, 20 HARV. J. LEGIS. 541, 548 n.40 (1983) (describing how one cable operator refused to carry a channel offering 24-hour news so that it could offer its own news channel instead).

<sup>64.</sup> See National Telecommunications and Information Admin., Video Program Distribution and Cable Television: Current Policy Issues and Recommendations 89-107 (1988). The National Telecommunications and Information Administration found no serious threat to competition by vertically-integrated companies' refusal to deal. It is possible, however, to be more skeptical and concerned about anti-competitive actions. The report describes instances such as the sudden turn-around when the Cable News Network adopted a policy against selling multichannel, multipoint distribution systems shortly after several cable operators acquired a financial interest in its parent company. The report also ignores the issue of whether new competitors for existing cable programs will ever start, knowing that to survive they must gain access to systems that own the very services with which they want to compete.

panies to adopt prior to offering enhanced services. The Justice Department guidelines facilitate understanding of the components of an ONA. The Justice Department defined ONA as a regime that "encourages dominant carriers to implement technological change that, by decreasing competitive risks, will reduce the need for regulation." At the heart of this architecture, transmission of information is transparent. Such transmission is open to all service providers making discrimination by the carrier difficult or impossible, and is designed to make detection of carrier cross-subsidization simple. The underlying technology makes the system accessible and refusals to deal obvious. Any authorization for IBNs should include a similar architectural requirement.

Moreover, specific policies requiring open access should be in place before the IBN system is built. Whether the IBN operator is permitted to offer programming and information services, or is able to enter into exclusive lease arrangements with service providers, an incentive to discriminate against other providers would be present. There should be an explicit requirement that the IBN offer service to all customers on a non-discriminatory basis. To No IBN operator should be permitted to harm a direct or indirect competitor either by denying service or offering inferior service. Creating a system in which, unlike the cable industry, programs and services only survive when marketplace demand for them exist, and not simply because they are protected from competition by the monopoly conduit, is socially desirable and economically efficient. Additionally, those entering the business of operating an IBN system should know at the outset that profits will not come from anti-competitive practices.

#### VI. WHOSE SPEECH IS IT?

A final issue for consideration is whether the speech, data and programming that an IBN carries must be attributed to the IBN operator, even when an unaffiliated entity furnishes the information to the IBN. Should the IBN operator be legally responsible for illegal, libelous and otherwise undesirable material that it does not produce, but carries over its wires?

<sup>65.</sup> Amendment of Sections 64.702 of the Commission's Rules and Regulations, CC Docket No. 85-229, *Report and Order*, 104 FCC 2d 958 (1986) ("Computer III"). AT&T was largely excused from these requirements in 2 FCC Reg. 3035 (1987) ("Phase I Recon Order").

<sup>66.</sup> Computer III, 104 FCC 2d at 1063.

<sup>67.</sup> Id.

<sup>68.</sup> Id.

<sup>69.</sup> Id., 104 FCC 2d at 1063.

<sup>70.</sup> See supra note 58, at 57.

Some telephone companies have been warned that they are responsible for the services they carry. A local prosecutor threatened Mountain Bell with prosecution for carrying a dial-a porn service in violation of state law barring the distribution of explicit sexual material to minors.<sup>71</sup> Consequently, Mountain Bell immediately discontinued the service.<sup>72</sup>

In contrast, cable operators, who have been barred from interfering with the public access programs, are immunized against liability for such programming. 73 A court found an early FCC rule, making cable operators liable for carrying obscene access programs, unconstitutional because the FCC rule forced the operator to serve as, "both judge and jury, and subjected the cable user's first amendment rights to decision by an unqualified private citizen."<sup>74</sup>

To avoid the recurrence of unqualified censorship, IBN operators need similar protection. A wide range of concerns about speech can be raised; such as libel, obscenity, invasion of privacy, disclosure of trade secrets, and incitement.

The IBN operator is not capable of prescreening all communication to determine the propriety of content. Moreover, the operator is not qualified to make the exceedingly difficult legal judgments concerning when protected speech crosses the line to illegality. Thus, each individual programmer and service provider should be held strictly liable for the communication they produce. In contrast, IBN operators should only be accountable for the programming they control.

#### VII. CONCLUSION

The Supreme Court stated that, "Each method of communicating ideas is a law unto itself, and that law must reflect the differing natures, values, abuses, and dangers of each method."<sup>75</sup> This principle should direct policy makers, as well as constitutional adjudication. The technology and economics of IBNs require a legal framework that is sensitive to their nature. Regulators need not reinvent the wheel or wait for crises to arise. Our previous experience with other forms of

<sup>71.</sup> Carlin Communications v. Mountain State Tel. & Tel., 827 F.2d 1291, 1293 (9th Cir. 1987).

<sup>72.</sup> Murphy, Phone Firms Can Ban "Dial-a-Porn" Lines, Court Says, L.A. Times, Sept. 15, 1987 at 3.

<sup>73. 47</sup> U.S.C. §§ 531(e), 558 (Supp. 1987).

<sup>74.</sup> Midwest Video Corp. v. FCC, 571 F.2d 1025, 1057 (8th Cir. 1987), affd on other grounds, 440 U.S. 689 (1979).

<sup>75.</sup> Metromedia, Inc. v. City of San Diego, 453 U.S. 490, 501 (1981) (quoting Kovacs v. Cooper, 336 U.S. 77, 97 (1949) (Jackson, J., concurring)).

electronic communication not only illustrates the dangers that could engulf IBNs, but the possible solutions as well.

Preliminary pro-competitive, pro-diversity, pro-privacy and pro-security measures can be implemented before the first electronic wave floats across the broadband cable. These measures will enhance business planning by those involved in the industry, encourage trust in the system by others, and avoid unnecessary and wasteful repetitions of previously fought legal battles. History can be our guide for creating a legal framework that will permit IBNs to reach their full potential.