NEW YORK LAW SCHOOL

NYLS Journal of International and Comparative Law

Volume 19
Number 3 *Volume 19 Number 3 2000*

Article 5

2000

INTERNET INDECENCY, INTERNATIONAL CENSORSHIP, AND SERVICE PROVIDERS' LIABILITY

Mark Konkel

INTERNET INDECENCY, INTERNATIONAL CENSORSHIP, AND SERVICE PROVIDERS' LIABILITY

I. INTRODUCTION

Ironically, Felix Somm's conviction troubled even his prosecutors.[1] Somm was the Managing Director of CompuServe Deutscheland Gmbh ("CompuServe Germany"), a large Internet Service Provider ("ISP") which operated as a subsidiary of CompuServe USA.[2] In late 1997,[3] the Local Court of Munich charged that Somm intentionally provided German Internet users with access to "violent, child, and animal pornographic representations"[4] and to three computer games that, because of their violent content, were banned under German law.[5] According to the Local Court, German Internet users were able to procure the illegal material, which had been stored in newsgroups,[6] via Internet access provided by CompuServe Germany.[7] Thus, although CompuServe Germany "was not technically able to block [the] newsgroups in question,"[8] the Local Court charged that Somm

---

1. Prosecutors in the case of Felix Somm themselves, in fact, "swung over to the view that Somm was not liable . . . and had called for him to be acquitted." *Prosecutors Have Change of Heart in Internet Case,* ORLANDO SENTINEL, June 4, 1998, at A16. *See also Prosecutors Appeal German CompuServe Porn Conviction,* NETWORK BRIEFING, June 4, 1998, at 1.

2. *See* Hans-Werner Moritz, *Pornography Prosecution in Germany Rattles ISPs,* NAT'L L.J., Dec. 14, 1998, at B7.

3. *See id.*

4. *Judgment of the Local Court Munich in the Criminal Case Versus Somm, Felix Bruno,* (visited Mar. 10, 2000) translated at <http://www.cyber-rights.org/isps/somm-dec.htm>, II.1. A full copy of the actual decision in German is viewable in Adobe Acrobat format at <http://www.jura.uni-wuerzburg.de/sieber/somm/somm-urteil.pdf> (visited Mar. 10, 2000).

5. *See id.* at IV.2.

6. "[N]ewsgroups, or discussion groups as they are often labeled these days, consist of people discussing various issues. Similar to email lists, newsgroups cover a wide variety of interests. . . . [N]ewsgroups are broadcast for anyone to read." Greg Notess, *On the Net,* 4 ONLINE 22, at 74. Data can be posted and archived in newsgroups in the form of text, images, or other data files. *Id.*

7. *See Somm, supra* note 4, at IV.1.

8. *Id.* at II.1.

and the corporation he managed had violated German criminal[9] and civil[10] laws by "assist[ing] in the dissemination of pornographic writings"[11] and negligently failing to block access to the censored games.[12]

What made these grave charges particularly disconcerting was what Felix Somm did *not* do: he did not, of course, post the officially censored images or games to the newsgroups.[13] Far from originating the illegal material, Somm could not even exercise direct control over much of the content of CompuServe's network.[14] Indeed, early in the government's inquiry, when investigators informed Somm of the presence of the illegal material on CompuServe's newsservers,[15] Somm promptly exercised what little content-control he could by immediately informing CompuServe USA of the presence of the material.[16] CompuServe USA responded by closing off all access to the newsgroups in question.[17]

This solution—the wholesale blocking of newsgroups in which illegal material had appeared—could be only temporary for two reasons. First, although some illegal material had been found in the newsgroups, those same newsgroups also contained perfectly legal material[18] to which customers demanded immediate access.[19] CompuServe customers in the United States

---

9. *See id.* at IV.1.

10. *See id.* at IV.2. Under the Act on Publications Deemed Morally Harmful to Youth, § 3 GjS, 52 StGB, the German government produces an index of publications that are banned for their morally harmful content. *Id.* In Germany, three video games accessible via CompuServe Germany had been included in the index due to their "social-ethical disorientation (including, but not limited to, realistically reproduced killings)." *Id.* at II.2.

11. *Id.* at IV.1. The illegal images were located in CompuServe newsgroups. Some of the newsgroups in question, such as alt.sex.pedophilia, alt.sex.pedophilia.boys, alt.sex.pedophilia.girls, alt.sex.incest, and alt.sex.bestiality.barney, would appear to be devoted entirely to illegal images. Other newsgroups, however, such as alt.sex and alt.erotica, contained mostly legal material. *Id.*

12. *See id.* at IV.2. The games in question were Doom, Heretic, and Wolfenstein 3D. *See id.*

13. This proposition, in fact, was Somm's first argument in his defense. *See id.* at V.

14. *See id.* at II.1. Interestingly enough, both the Local Court Munich and Somm agreed that Somm could exercise no direct physical control over the content provided by CompuServe USA. *See also* Kenneth Cukier, *PSINet Sends Warning Signals to German State*, COMM. WEEK INT'L, July 20, 1998, at 16 (noting that an "ISP is powerless to prevent users from accessing content that may be illegal under German law.").

15. *See Somm, supra* note 4, at II.1.

16. *See id.*

17. *See id.*

18. *See id.* at V.

19. *See* Moritz, *supra* note 2, at B7 (stating that "[p]ublic reaction to the newsgroups' suspension was overwhelmingly negative. Initially, CompuServe was branded a censor.").

and Germany thus protested vociferously when the ISP limited their access to this lawful content.[20] With pressure mounting against CompuServe to reopen the blocked newsgroups, the ISP soon restored full access.[21]

Second, CompuServe could not prevent the reappearance of illegal material on its network because CompuServe users, not the ISP itself, controlled the content of the newsgroups.[22] Certainly, the storage space in which some of the illegal data were found was technically under the physical control of CompuServe USA.[23] CompuServe Germany, however, merely provided access to these and other newsgroups in which any "third party" Internet user could post any material at any time, whether the user purchased Internet access from CompuServe or not.[24] With millions of Internet users worldwide,[25] CompuServe found it impossible to police its storage space against all material that might be illegal in some jurisdiction in the world.[26] Not surprisingly, then, more material banned under German law appeared soon after the newsgroups were reopened.[27]

Despite this lack of control over Internet content, the Local Court of Munich accused Somm of failing to comply with German law.[28] Thus, although Somm possessed no direct technical control over the newsgroups and positively no control over the material posted by individuals therein, he was convicted, fined substantially, and given a two-year suspended sentence.[29]

Traditionally, concern over the criminalization of Internet content has been regarded as the domain of civil libertarians and others committed to free

---

20. *See id.*

21. *See id. See also Somm, supra* note 4, at II.1.

22. Somm himself made this commonsensical argument: the illegal material identified in the indictment "[came] from third parties." *Somm, supra* note 4, at V. Ironically, the Local Court also acknowledged this third-party control. *See id.* at II.1.

23. *See id.* at II.1.

24. *See id.* Somm argued in his defense, for example, that CompuServe, "through its data lines, allowed access [to the materials in question] which were stored in other computer systems." *Id.*

25. *See China: 1.18 Million Surf Internet*, CHINA DAILY, July 15, 1998, at 1 (predicting 250 million Internet users worldwide by 2000).

26. *See Executive Convicted over Internet Porn*, FACTS ON FILE WORLD NEWS DIGEST, June 25, 1998, at E2 (noting that "[s]everal experts had testified that it was not possible for an Internet service to block all such [illegal] material.").

27. *See Somm, supra* note 4, at II.1.

28. *See id.* at IV.1.A.3.b.

29. *See id.* at VI. The fine amounted to 100,000 German marks, or about $57,000. *See Executive Convicted over Internet Porn, supra* note 25, at E2.

expression online.[30] The Somm case, however, starkly demonstrates a concern for ISPs as well. Clearly, as Somm himself argued unsuccessfully,[31] the Local Court of Munich misunderstood the level of control that ISPs are able to exercise over the content available on the Internet, content generally created by individual users, not by the ISP that provides Internet access.[32] No large ISP could ever effectively police the activities of the millions of individual users on the Internet each day.[33] Thus, CompuServe could prevent all criminal content from appearing within its newsgroups only by blocking access altogether.[34] Such a solution, however, even if effective in keeping out illegal material, would drive away customers: the content of a newsgroup might be illegal in one jurisdiction, but perfectly legal and demanded by valuable customers in another jurisdiction.[35]

The danger that the Somm case represents, then, has to do with an ISP's lack of proprietary control over information appearing on the Internet. The Internet is a large, global network, the content of which is the product of users who could be located anywhere in the world.[36] Indeed, as the U.S. Supreme Court noted in a landmark case, "[t]he content on the Internet is as diverse as human thought."[37] As a result, the officers of access providers like CompuServe cannot constantly be aware of network content.[38] But when corporate officers are held personally responsible for the acts of third parties over whom they have no control, those officers arguably are exposed to a kind of strict liability: they face civil and criminal penalties for acts over

---

30. *See, e.g.*, Global Internet Liberty Campaign (GILC), *Regardless of Frontiers: Protecting the Human Right to Freedom of Expression on the Global Internet* (visited Mar. 10, 2000) <http://www.gilc.org/speech/report>; American Civil Liberties Union (visited Mar. 10, 2000) <http:// www.aclu.org/issues/cyber/hcml.html>; Electronic Frontier Foundation (visited Mar. 10, 2000) <http://www.eff.org>.

31. *See Somm*, *supra* note 4, at V.A. (arguing that Somm did not originate the material, did not store the material on the CompuServe network, and made "every reasonable effort to prevent the retrieval and storage of criminal content").

32. *See Regardless of Frontiers*, *supra* note 30, at 6–7 (arguing that the Internet, because users have numerous ways of circumventing government controls, is almost entirely "user-controlled.").

33. *See China: 1.18 Million Surf Internet*, *supra* note 25, at 1.

34. *See Somm*, *supra* note 4, at II.1. When, for example, alt.sex.erotica was closed, no CompuServe user could visit the newsgroup until it was later reopened by CompuServe. *Id.*

35. This was true in the case of Somm, for example, where the censored games were proscribed under German law but perfectly legal to possess and share in the United States, where they probably originated. *See Somm*, *supra* note 4, at IV.2; *see also infra* Part III.A.

36. *See Regardless of Frontiers*, *supra* note 30, at A.

37. American Civil Liberties Union v. Reno, 521 U.S. 844, 852 (1997)(citing American Civil Liberties Union v. Reno, 929 F.Supp. 824, 842).

38. *See* Moritz, *supra* note 2, at B7; *see also Somm*, *supra* note 4, at V.B.

which they have little, if any, actual awareness.[39] To complicate matters, no international treaty or agreement establishes a single international standard of liability for ISPs.[40] In order to provide access to the Internet content that users lawfully demand, transnational ISPs must run the risk of criminal liability in a world where many forms of expression are censored.[41]

Thus, international law has yet to catch up with the market realities–and certainly the technical realities–of the Internet. As long as there is no international standard of protection that reflects the low level of ISP involvement in the creation of Internet content, transnational service providers face at least two distinct problems. First, as the *Somm* case makes clear, ISPs will generally find it difficult to comply with local laws banning certain material because an ISP cannot control the millions of users on the Internet.[42] As a result, such corporations will face a significantly greater cost of doing business as they attempt to police information over which they have little or no proprietary control.[43] Second, and more alarmingly, transnational ISPs will be unable to shield their officers from unwarranted criminal and civil liability without the protection of such international standards.[44] There is a clear need for a multilateral treaty, the first of its kind,[45] designed to protect ISPs from liability for communications made by third parties.

This note proposes that a multilateral treaty regulating the level of ISP liability for third-party acts is crucial to encouraging the development of international commerce on the Internet. Without such international agreement on an appropriate level of ISP liability for third-party acts, corporations face a discouraging uncertainty in "a unique and wholly new medium of worldwide human communication."[46] Sovereign nations will, of course, retain the power to make laws regulating the speech or other expression of its citizens.[47] One thing is certain, however: liability for

---

39. A perfect illustration is the Somm case itself, of course, where the Court imposed criminal sanctions against Somm even though the Court admitted that CompuServe Germany could not have blocked or removed the illegal material. *Somm, supra* note 4, at II.1.

40. *See* discussion *infra* Part III.C.

41. *See* discussion *infra* Part III.B.

42. *See China: 1.18 Million Surf Internet, supra* note 25, at 1.

43. As Somm and CompuServe argued, "in at least 99.9% of its data traffic . . . CompuServe GmbH provided access to lawful content." *Somm, supra* note 4, at V.B.

44. *See* discussion *infra* Part III.

45. *See* discussion *infra* Part III.

46. American Civil Liberties Union v. Reno, 521 U.S. 844, n.4 (1997) (O'Connor, J., concurring in part and dissenting in part).

47. Even international treaties designed to protect expressive rights nonetheless explicitly recognize that individual rights to expression may be limited by the legitimate exercise of the

prohibited acts of expression will threaten the viability of doing business as an ISP in a world of differing standards for the protection of speech.[48]

II. THE *SOMM* CASE

The case against Felix Somm embodies certain misconceptions about an ISP's control over Internet content. Uncorrected, these misconceptions will put ISPs at risk of criminal sanctions wherever foreign jurisdictions illegalize at least some forms of expression.[49] In the *Somm* case, the Local Court of Munich found Somm criminally liable for the acts of Internet users even though he was not aware of the presence of illegal material[50] and "had no opportunity to exercise influence on the data storage device of CompuServe USA."[51] Somm and CompuServe Germany were therefore penalized for failing to achieve the unachievable task of preventing any and all illegal material from ever becoming available to CompuServe users in Germany.[52]

A. Background to the Somm *Case*

In November of 1995, German investigators notified Felix Somm that several images depicting child pornography and bestiality, among other legal pornography, had been found in CompuServe newsgroups.[53] Investigators further alleged that they had accessed three violent war games on the

---

state's police power in order to protect public health, safety, or welfare. *See* discussion *infra* Part III.C. *But cf.* Amy Harmon, *Internet Tests Boundaries of Decency and Nations Computers: Cyberspace May be Making Laws of Any One Country Irrelevant, Shifting Power From Governments*, L.A. TIMES, Mar. 19, 1997, at A1 (noting that legal scholars and "crypto-anarchists" predict that "cyberspace will ultimately render the nation-state as we know it irrelevant, with law rooted in physical control of geographic territory giving way to new forms of governance springing from online communities").

48. Governments frequently view restriction of Internet content as important to enforcing morality and preventing the use of Internet technology for "subversive" ends and "antigovernment activities." *See* Seydou Amadou Oumarou & Rene Lefort, *The Web, the Spider, and the Fly*, UNESCO COURIER, Sept. 1, 1998, at 38.

49. *See id.*

50. *See Somm*, *supra* note 4, at V.B.

51. *Id.* at IV.1.B.2.c.aa.

52. The task is unachievable precisely because the lack of meaningful geographical boundaries on the Internet and the resulting ability of users to post any information from any location makes it impossible to monitor the origin or location of all material on the Internet. *See* Harmon, *supra* note 47, at A1 (arguing that the Internet is "blind to the territorial boundaries tha have traditionally dictated legal jurisdiction.").

53. *See Somm*, *supra* note 4, at II.1.

CompuServe USA network.[54] Although the material was stored as data on the CompuServe USA network, third parties could and did post data to the network.[55] Thus, the specific content available in the newsgroups was not created or maintained by Somm, CompuServe Germany, or CompuServe USA.[56] CompuServe USA, as with any ISP, could not actually prevent users from posting images; rather, it could only block all users' access to an entire newsgroup which allegedly contained illegal material.[57] CompuServe Germany had even less technical control: it solely provided individuals with access to CompuServe USA's server.[58] When investigators informed Somm of the offending newsgroups,[59] Somm took the only action he could. In December 1995, he asked CompuServe USA to block all users' access to the newsgroups containing illegal material, which it did.[60]

CompuServe USA, however, would not block access to the newsgroups for long. As CompuServe USA quickly discovered, there was tremendous backlash from CompuServe users in America and elsewhere who were prepared to take their business to another service provider if CompuServe, by blocking an entire newsgroup, limited their access to legal expression.[61] In February of 1996, CompuServe USA accordingly reopened a majority of the blocked newsgroups.[62]

Somm and CompuServe USA, however, did not simply abandon any attempt to comply with German law. Rather, as noted in a letter posted to the CompuServe network, CompuServe had made available blocking software that would allow individual users to block their own and their children's access to illegal material.[63] In doing so, CompuServe hoped to demonstrate both its willingness to abide by German law and its commitment to providing

---

54. *See id.* at II.2. These games included Doom, Heretic, and Wolfenstein 3D. *Id.*

55. *See Somm, supra* note 4, at V.A.

56. *See id.* at IV.1.A.3.b (where the Local Court itself notes that CompuServe Germany "does not make available for use third-party content, but only connects customers of CompuServe USA in Germany . . . with the parent company." *Id.*

57. *See* Moritz, *supra* note 2, at B7 (observing that since "it was not technically feasible at that time to suspend access exclusively in Germany . . . CompuServe Inc. was compelled to suspend access to the newsgroups for all of its more than 4 million members globally.").

58. *See Somm, supra* note 4, at IV.1.B.2.a.

59. *See id.* at II.1.

60. *See id.*

61. *See* Moritz, *supra* note 2, at B7 (observing that "[p]ublic reaction to the newsgroups' suspension was overwhelmingly negative").

62. *See Somm, supra* note 4, at II.1.

63. *See id.*

its users elsewhere with continuing access to its newsgroups.[64] The blocking software, the letter noted, "allow[ed] CompuServe to take youth protection seriously and simultaneously to re-open most of the temporarily blocked newsgroups,"[65] and therefore to satisfy the legitimate demands of both German law and CompuServe's non-German customers.

Shortly after the newsgroups were reopened, investigators again discovered that material prohibited by German law was accessible to Germans through the CompuServe network.[66] In late February 1996, the Regional Court for the District of Munich 1 notified Somm that he was still providing access to material then prohibited by two sections of the Penal Code[67] and by the Act on the Dissemination of Publications Morally Harmful to Youth.[68] Finally, charges were brought against Somm, CompuServe Germany, and CompuServe USA for "mak[ing] publicly accessible pornographic writings containing acts of violence, sexual abuse of children and sex acts between human beings and animals" in violation of two sections of the German Penal Code.[69] Moreover, the Local Court alleged that Somm had negligently violated the Act on the Dissemination of Publications Morally Harmful to Youth in making available the war games, which were listed on an index of banned publications.[70]

Since the Local Court did not allege that Somm had published the illegal material himself, these criminal charges rested on several key legal assumptions. The Local Court charged Somm as an accomplice to the criminal act of making available illegal material simply by providing access to the CompuServe USA network.[71] Although the Local Court would find that "viewed individually, CompuServe Germany and the accused had no opportunity to exercise influence on the data storage device of CompuServe USA,"[72] it nonetheless maintained that Somm and CompuServe intended to circulate the illegal images.[73] As to the illegal games, the Local Court reasoned that "it was within [Somm's] competence to observe that German laws were complied with. Therefore, it was within his duty of reasonable

64. *See id.*
65. *Id.*
66. *See id.*
67. *See id.*
68. *See id.*
69. *Id.* at IV.1.
70. *See id.* at IV.2.
71. *See id.* at IV1.A.3.
72. *Id.* at IV.1.B.2.a.
73. *See id.* at IV.1.A.3.b.

care to ensure that no indexed games were offered to customers in Germany."[74]

B. Somm's Defense

At trial, Somm made several arguments in his defense that would appear to be common sense to anyone with even casual knowledge of the Internet. First, Somm argued that in immediately requesting that CompuServe USA block access to the newsgroups in question, he had taken the only steps towards direct technical control over the illegal images and games that he could.[75] Given Somm's subsequent conviction, it is startling to observe that the Court agreed with Somm: in the absence of user-based blocking software, only CompuServe USA could effectively block or limit access to any newsgroups.[76]

Somm also argued that he was not the "originator" of the images in question and that, rather, the information had been posted by third parties.[77] In fact, Somm alleged, many of the images and texts identified in the indictment were never stored on computers owned by CompuServe Germany or its parent company.[78] Instead, CompuServe merely provided access to those images and data which were actually stored, in many cases, in other computer systems accessible via the Internet.[79] In any case, Somm argued, "in at least 99.9% of all [CompuServe Germany's] traffic data . . . [it] provided access to lawful content."[80]

Somm's defense was thus simple and direct: the illegal content was not created or distributed by Somm, but rather by third parties to the action, parties over whom Somm had no control.[81] Consequently, Somm exercised what little control over content he could by immediately asking CompuServe USA to remove the offending material.[82]

As sensible as they were, these arguments did not sway the court. On the charge that Somm and CompuServe Germany distributed pornographic material, it did not matter if Somm did not post and was not specifically

---

74. *Id.* at IV.2.
75. *See id.* at V.B.
76. *See id.* at II.1.
77. *See id.* at V.A.
78. *See id.*
79. *See id.*
80. *Id.* at V.B.
81. *See id.* at V.A.
82. *See id.* at V.C.

aware of the posting of illegal images; since Somm and CompuServe Germany were aware that the images were stored in CompuServe USA's storage space and nonetheless provided access, it was their "intent" that the images be distributed.[83] As to Somm's liability on the charge of distributing the war games, the Court did not have to allege that Somm actually knew about the illegal material. Rather, Somm's liability rested on a negligence standard.[84] In the Court's view, "it was within [Somm's] duty of reasonable care to *ensure* that no [illegal] games were offered in Germany."[85]

Among the possible implications of finding an ISP or one of its officers criminally liable for acts they could not prevent or meaningfully control, two are particularly disturbing. On the one hand, the court may have believed that Somm and CompuServe Germany had more control over the activity of users on their network than they actually did.[86] If this were true, then Somm's criminal liability would rest on the erroneous assumption that Somm had personally contributed to the criminal act by his knowing failure to exercise available controls to regulate the content of the CompuServe newsserver. On the other hand, if the court did fully recognize that Somm exercised no control over the acts of individual users, then it was nonetheless willing to attribute liability without a showing that Somm had personally committed any fault.[87]

---

83. *See id.* at IV.1.3.b.

84. *See id.* at IV.2.A.5.

85. *Id.* (emphasis added).

86. That is, even the court noted that CompuServe Germany "only connects the customers of CompuServe USA in Germany . . . with the parent company." *Id.* at IV.1.B.2.a. Moreover, Somm argued that even if he could control the postings of CompuServe users, "the images and texts identified in the indictment could have been procured in identical manner via any of the approximately 300 access providers presently operating in Germany." *Id.* at V.B. The Court blandly asserted that the accessibility of images from other ISPs was "of no relevance to the case." *Id.*

87. This is so because the court found Somm liable even though it agreed that Somm may have had nothing more than constructive notice of acts taken by third parties. *See id.* at IV.1.B.2.c.aa.

C. *Aftermath of the* Somm *Case*

Naturally, Somm's conviction provoked widespread public concern over holding ISPs criminally liable for acts taken by users.[88] Indeed, the *Somm* case created enough alarm to cause at least one ISP to withdraw from the German market.[89] In the midst of the Somm prosecution itself, the German legislature attempted to stave off what was increasingly regarded as an unwise and unfair prosecution[90] by passing an amendment to the Information and Communications Services Act,[91] which regulates German telecommunications businesses, including ISPs.[92] This amendment was designed to shield service providers like CompuServe and corporate officers like Somm from criminal or civil liability for acts taken independently by their users.[93]

However, the Judge was not moved by this development.[94] Although the amendment to German law apparently contemplates a general lack of the ability of service providers to block content unpredictably posted by its users, according to the Local Court of Munich, "[t]he liability of the accused [was not] limited" by the Act.[95]

In a gesture as unusual as that of the legislature, the prosecutors in Somm's case were sufficiently uncomfortable with the nature of the judge's rationale to appeal the case themselves.[96] As one article notes, "[e]ven government prosecutors had acknowledged that Somm could not be held responsible for the illegal material."[97] Somm's appeal was ultimately

---

88. This was especially alarming to German ISPs, of course. *See* Cukier, *supra* note 14, at 16 (observing that "German Internet executives are wary that federal officials intend to . . . hold ISPs liable" regardless of new laws designed to shield ISPs from liability); *see also* Moritz, *supra* note 2, at B7 (reporting that Somm's "prosecution sent shock waves through the German high-tech industry").

89. *See* Cukier, *supra* note 14, at 16. ("PSINet Germany GmbH will move a significant portion of its web-hosting business outside of Germany").

90. *See generally id.*

91. *Informations-und Kommunikations dienste-luKDG (Teledienstegesetz [TDG])* art. I, § 5(1) (F.R.G.). This section holds ISPs liable only for that content "which they make accessible for use." *Id.*

92. *See* Moritz, *supra* note 2, at B7.

93. *See* Cukier, *supra* note 14, at 16 ("Germany's Multimedia Act . . . seeks to protect ISPs from liability from content they themselves do not host.").

94. In rendering his decision, the judge averred that "there can be nowhere outside the law on the Internet." *Executive Convicted over Internet Porn, supra* note 25, at E2.

95. *Somm, supra* note 4, at IV.1.B.

96. *See Prosecutors Appeal German CompuServe Porn Conviction, supra* note 1, at 1.

97. *Executive Convicted Over Internet Porn, supra* note 26, at E2.

successful; the appeals court "agreed with Somm that he had only provided German customers with access to the information available on Compuserve USA servers and could not be considered as an accomplice to the distribution of illegal materials."[98] Even if the success of Somm's appeal has vindicated the German law that protects ISPs from liability, however, Somm's case raises the specter of similar prosecutions in other jurisdictions. As one commentator noted, "this ruling has swept away much legal certainty for Internet Service Providers .... ISPs across the globe have every reason to be nervous and unsure about liability in the future."[99]

The *Somm* case illustrates perfectly what might deter ISPs from operating internationally: in the United States, where the "illegal" games almost certainly originated, the games are not illegal and may even be constitutionally protected speech.[100] Thus, Somm's liability rested on acts, taken without his knowledge, that were legal where they happened. In the absence of any international standards to shield ISPs from this unwarranted liability, the scope of the problem is extensive: across all jurisdictions in the world where Internet access might exist, any number of forms of sexual, political, and artistic expression are prohibited by national governments.[101] If corporate officers can be held liable whenever third parties post material that is illegal in some jurisdiction in the world willing to prosecute, corporations might choose to abandon a market rather than face the cost and futility of policing the massive amount of information to which they provide access.[102] Without legal safeguards for ISPs, differing international standards for the protection of expression will burden ISPs with a very expensive, and probably impossible, duty.

---

98. John Schmertz & Mike Meier, *German Appeals Court Reverses Conviction of Former Compuserve Manager for Allegedly Facilitating Telegraphic Disctirubtion of Pornography Through Internet*, 5 INT'L LAW UPDATE 12 (1999).

99. Moritz, *supra* note 2, at B7.

100. *See* discussion *infra* Part III.A.

101. *See* discussion *infra* Part III.B.

102. As one Canadian ISP spokesperson suggested, "[t]he average ISP is not able to check content; it's quite simply not our job. We are simply transferring the [information]." Laura Lyne McMurchie, *Proposed Internet Bill Product of Naïve Mind*, COMPUTING CANADA, Aug. 17, 1998, at 8. *See also* Cukier, *supra* note 14, at 16.

III. INTERNATIONAL STANDARDS FOR THE PROTECTION OF EXPRESSION

As the *Somm* case illustrates, the imposition of liability on ISPs for the communications of individual users is problematic for two reasons. First, there is a general inability on the part of ISPs to regulate Internet content.[103] Second, differing jurisdictional standards for the protection of speech or expression creates tremendous potential for undeserved criminal and civil penalties.[104] That is, although a particular image or text could be considered protected expression in one jurisdiction, and therefore legal, the same image or text could be prohibited by law in another jurisdiction.[105] In the absence of broad international standards designed to protect ISPs from liability, service providers could be held liable for the dissemination of prohibited expression whenever one of its thousands of users posts material that is censored in any jurisdiction, even if the same material is legal in the user's own jurisdiction.[106]

This problem is hardly imaginary: international legal standards for the protection of expression vary widely. Given that the Internet possesses no meaningful national boundaries,[107] the lowest standards for the protection of speech are those most likely to create a wide range of illegal expression that will be of greatest concern to ISPs doing business overseas.[108] Although expression receives comparatively broad protection in the United States and some other Western democracies,[109] many nations currently prohibit a wide range of speech.[110]

---

103. *See* Harmon, *supra* note 47, at A1.

104. *See* discussion *infra* Part III.

105. The Somm case is a good illustration: there, the games that formed part of the basis of Somm's criminal liability, although illegal in Germany, are not proscribed (and are probably even protected) by American law. *See id.*

106. *See id.*

107. *See* Harmon, *supra* note 47, at A1 ("[I]n cyberspace, there is no distance between two points").

108. *See* Oumarou & Lefort, *supra* note 48, at 38 (noting that the "monitoring of content . . . would require . . . at least a lowest common denominator").

109. *See* discussion *infra* Part III.A.

110. *See* discussion *infra* Part III.B. Even in such nations, however, an issue of content control arises because of "an increased availability of objectionable material." Kim Rappaport, *In the Wake of Reno v. ACLU: The Continued Struggle in Western Constitutional Democracies with Internet Censorship and Freedom of Speech Online*, 13 AM. U. INT'L L. REV. 765 (1998). Rappaport adds that "[a]s a result, some governments have taken steps to implement restrictions at the national level. The United States and Germany are the most notable examples, having sparked a flurry of legislative and legal battles over how to regulate

A. Internet Service Provider Liability in the United States

The First Amendment to the United States Constitution has been interpreted by the United States Supreme Court as establishing broad protections for many forms of speech and individual expression, subject to certain limitations discussed below.[111] The Supreme Court has repeatedly held that at the core of the First Amendment lies a commitment to the notion that the government may not prohibit speech based on the content of its message.[112] One commentator has argued that this historical protection of content-based speech reflects the Framers' intention to protect not only political speech,[113] but other forms of expression since "virtually everything from comic strips to commercial advertisements to even pornography can have a political dimension."[114]

1. General Protections for ISPs

American cases involving the liability of Internet service providers for information or material posted through its network to the Internet have generally revolved around issues of copyright infringement[115] or defamation.[116] In such cases, the consequences are civil and proceed not from government attempts to restrict speech per se but rather from the distinct legal principles of copyright infringement[117] and of defamation.[118] Both causes of action seek to compensate aggrieved parties for economic or

---

this evolving medium." *Id.*

111. One eminent scholar notes that the "Supreme Court has never accepted the view that the First Amendment prohibits all regulation of expression." ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES § 11.1.2 (Aspen Law & Business 1997).

112. *See, e.g.*, Police Dep't of Chicago v. Mosley, 408 U.S. 92, 95 (1972) (holding that content-based regulation of speech "is never permitted.").

113. *See* CHEMERINSKY, *supra* note 111, § 11.1.2.

114. *Id.*

115. *See, e.g.*, Playboy Enter. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993) (involving copyright infringement); Playboy Enter. v. Starware Publishing Corp., 900 F. Supp. 443 (S.D. Fla. 1995) (involving copyright infringement); Central Point Software v. Nugent, 903 F. Supp. 1057 (E.D. Tex. 1995) (involving copyright infringement).

116. *See generally* Zeran v. America Online, 129 F.3d 327 (4th Cir. 1997) (involving a defamation claim against an American ISP for speech initiated by a third party).

117. *See generally* Playboy Enter. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993); Playboy Enter. v. Starware Publishing Corp., 900 F. Supp. 443 (S.D. Fla. 1995); Central Point Software v. Nugent, 903 F. Supp. 1057 (E.D. Tex. 1995); *Zeran*, 129 F.3d 327.

118. *See Zeran*, 129 F.3d 327.

personal injury, but do not seek to limit expression based on its political, sexual, or artistic content.[119]

2. American Civil Liberties Union v. Reno

One attempt in the United States to regulate Internet speech based on its content was the Communications Decency Act of 1996 ("CDA").[120] The CDA attempted to regulate, among other things, prurient content that children might access on the Internet.[121] Failure to remove such material or to block access would result in civil and criminal penalties.[122]

However, in *American Civil Liberties Union ("ACLU") v. Reno*,[123] the U.S. Supreme Court affirmed the decision of the District Court, which had struck down the CDA as unconstitutional.[124] The District Court had held that the Act unconstitutionally impinged upon established First Amendment protections of free speech.[125] In upholding that decision, the Supreme Court reasoned that limiting Internet content to protect minors would interfere with constitutionally protected adult communications.[126]

The stability of this area of constitutional law was confirmed by the failure of another attempt by the U.S. government to regulate speech on the Internet.[127] In October 1998, President Clinton signed a new federal cyber-censorship law known as the Child Online Protection Act.[128] Although the ACLU promptly challenged this so-called "CDA II" in a lawsuit named, appropriately, *ACLU v. Reno II*,[129] and although the judge issued a temporary

---

119. *See* Playboy Enter. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993); Playboy Enter. v. Starware Publishing Corp., 900 F. Supp. 443 (S.D. Fla. 1995); Central Point Software v. Nugent, 903 F. Supp. 1057 (E.D. Tex. 1995); *Zeran*, 129 F.3d 327.

120. *See* Communications Decency Act of 1996, 47 U.S.C. § 223 (1996).

121. *See, e.g.*, 47 U.S.C. § 223(d)(1996). This subsection of the CDA made it illegal for anyone to use an "interactive computer service" to send, among other things, any "communication that . . . depicts or describes . . . sexual . . . activities or organs." *Id.*

122. *See id.*

123. 521 U.S. 844 (1997).

124. *See id.* at 885.

125. *See id.* at 886.

126. *See id.* at 876

127. *See* 47 U.S.C. § 231 (1999).

128. *See* 47 U.S.C. § 231 (1999). This law would impose civil and criminal penalties on commercial disseminators of pornographic material who make such material available to children. *See id.*

129. 31 F.Supp.2d 473 (E.D. Pa. 1998).

injunction prohibiting the government from enforcing the law,[130] the U. S. Justice Department continues to defend it.

B. Internet Service Provider Liability in Other Countries

Many countries, however, do not provide protections for expression on the Internet similar to those offered in the United States or, more recently, Germany.[131] First, even among Western democracies, attempts to regulate Internet content are not uncommon and frequently revolve around notions of "indecent" expression.[132] During the same year as Somm's prosecution, for example, a bill known as the Internet Child Pornography Prevention Act was introduced in the Canadian House of Commons.[133] The legislation sought to control Internet content through ISP licensure requirements[134] and imposed criminal penalties on those who aided in the dissemination of child pornography.[135] Again, if ISPs are thought to "disseminate" images by unknowingly providing access to them, another criminal prosecution resembling Somm's is not unimaginable.

In many non-western nations, the range of speech subject to official censorship includes not only sexually oriented expression but also a wide range of political speech.[136] If the Internet has demonstrated a unique capacity to promote democracy,[137] governments wishing to suppress political dissent unsurprisingly turn to regulation of speech on the Internet in order to control political discourse.[138] The following section offers two examples of such control.

1. The Malaysian Example

The legal regulation of the Internet for political purposes in Malaysia is an excellent example of the criminalization of Internet speech by national governments. Late in 1998, state police in Malaysia "set up an Internet unit

---

130. *See id.* at 477.

131. *See* discussion *supra* Part III.A.1; *see also* Rappaport, *supra* note 110, at 765.

132. Both the original CDA and the so-called "CDA II" represent Congressional attempts to censor pornography that might be accessible to children on the Internet. *See* discussion *infra* Part III.A.

133. *See* McMurchie, *supra* note 102, at 8.

134. *See id.*

135. *See id.*

136. *See* discussion *infra* Part III.B.1.

137. *See Regardless of Frontiers*, *supra* note 30, at Part B.

138. *See* discussion *infra* Parts III.B.1–III.B.2.

[under Malaysia's Internal Security Act][139] to monitor sites and newsgroups that have been organizing protests against the jailing of the former Deputy Prime Minister, Anwar Ibrahim."[140] This police unit is also entrusted with the more ambiguously defined task of guarding against "information and messages [on the Internet] which could affect public security."[141] Although the government of Malaysia, under the leadership of current Prime Minister Mahathir Mohamad,[142] has denied political dissenters access to traditional media,[143] it is less able to control the abundant political discourse appearing on the Internet; thus, "Malaysians who feel their newspapers and broadcasters are toeing the government line too much have been turning increasingly to the Internet for alternative coverage."[144] Naturally, in nations subject to political instability, the range of political expression viewed as "affecting" public security could be quite broad.[145]

Indeed, Malaysia's net-censorship laws and policing have already effected the detainment and arrest of several Malaysian citizens "under the Internal Security Act after an anonymous e-mail warned that migrant workers from Indonesia were buying machetes as a prelude to riots."[146] These four citizens, characterized by Prime Minister Mohamad as "worse than cowards,"[147] may be held for up to two years without a trial.[148] Interestingly enough, the government tracked down the political dissenters mostly through the aid of Malaysian ISPs themselves, who presumably wished to avoid being accused of having helped to disseminate the rumors.[149] The risk of future criminal prosecutions is only increased by the great volume of political dissent now circulated via the Internet: the newsgroups and web pages in question were not simply "disseminator[s] of information" but acted as

---

139. *See, e.g.*, Chris Nuttal, *Malaysia's Net Patrol*, BBC ONLINE, (visited Oct. 27, 1999) <http://news2.thls.bbc.co.uk/hi/english/special%5Freport/1998/10/98/malaysia%5Fcrisis/newsid%5F186000/186753.stm>.

140. *Id.*

141. *Id.*

142. *See id.*

143. *See* Chris Nuttal, *Malaysians Take to Web in Anwar Protest*, BBC ONLINE, (visited Oct. 27, 1999) <http://news2.thls.bbc.co.uk/hi/english/sci/tech/newsid_181000/181991.stm>.

144. Nuttal, *supra* note 139.

145. This is especially the case with political dissent, which could merely be the expression of political opinion adverse to the government.

146. Nuttal, *supra* note 139.

147. Chris Nuttal, *Malaysia Arrests Net Newsgroup Suspects*, BBC NEWS ONLINE (visited Oct. 27, 1999) <http://news.bbc.co.uk/hi/english/sci/tech/newsid_149000/149273.stm>.

148. *See id.*

149. *See id.*

"campaign organiser" as well.[150] In response, the Inspector General of Police promised that "more arrests were imminent."[151]

2. The Chinese Example

In recent years, China has experienced a rapid expansion in its number of Internet users. Some reports indicate that the number of Internet users in China surpassed 1.18 million in the first six months of 1998.[152] As in other nations, the Internet has become an engine for the dissemination of political views in China.[153] Increasingly sensitive to and uncomfortable with the Internet's great potential to spread dissent, "Chinese police departments [have been] given the authority to monitor how individuals are using the Net."[154] For example, "a recent order has been released by the police and the Ministry of Culture's National Commercial Administration for tighter checks on China's growing number of Internet cafes."[155] By such legal action, the Chinese government is making concerted attempts to temper the increasing popularity of the Internet with sober warnings against fulminating political dissent: "[t]he order emphasized that Internet cafes were not allowed to engage in activities endangering state security or social stability, or criminal activities."[156] Such hostility to political speech on the Internet has resulted in the prosecution of one Chinese intellectual for the commission of crimes "aimed at subverting state political power."[157] Other such prosecutions are far from unlikely.[158]

Political dissent is not the only concern of the Chinese government. The recently outlawed Falun Gong religious sect has turned to the Internet to

---

150. *See* Nuttal, *supra* note 139.

151. Nuttal III, *supra* note 147.

152. *See China 1.18 Million Surf Internet*, *supra* note 25, at 1.

153. For example, China-based websites are frequently the source of "anti-American lashings and criticisms of Chinese leadership." Choo Li Meng, *Chinese Let Views Fly on Internet*, STRAITS TIMES (Singapore), July 1, 1999, at 40.

154. *Chinese Police to Patrol the Net*, NEWMEDIA CANADA, Jan. 26, 1999.

155. *China Warns Cybercafes Against Endangering State Security*, AGENCE FR.-PRESSE, Jan. 30, 1999.

156. *Id.*

157. *Chinese Intellectual Detained for Alleged Internet Crimes*, AGENCE FR.-PRESSE, Sept. 3, 1999.

158. Indeed, a recent circular distributed by Chinese police calls for "a crackdown on 'hostile elements' using the internet to foment political unrest." *Chinese Police Circular Calls for Crackdown on Internet Dissent*, AGENCE FR.-PRESSE, Sept. 1, 1999.

"spread rumors based on information in . . . ill-gotten state documents."[159] The police have actively investigated a number of such cases.[160] In fact, much as in Malaysia, the Chinese government has even begun to use the Internet itself to combat members of the sect, blocking or penetrating Falun Gong websites.[161] As the targeting of cybercafes and the Falun Gong sect demonstrate, with growing Chinese Internet use, the opportunity for ISPs to offend laws prohibiting political or other speech only increases.

C. International Agreements Protecting Expression

An apparent solution to the problem of transnational ISP liability for third-party acts lies in simply utilizing the broad language of certain human rights instruments aimed at protecting self-expression in order to constrict the range of criminally punishable expression.[162] At least three inadequacies arise with this solution, however. First, even under the terms of international agreements, a state would be able to restrict a wide range of speech pursuant to its police power, provided that it could claim that the expression imposed some danger to the health or welfare of its citizens.[163] Second, international instruments protecting freedom of expression do not generally have the status of binding law because they embody normative ideals[164] and establish limited enforcement mechanisms, if any.[165] Finally, and most simply, not all nations are signatory to these international accords.

---

159. *Falun Gong Followers Leak State Secrets*, XINHUA NEWS AGENCY, Oct. 25, 1999, at 1.

160. *See id.*

161. *See China's War with Falun Gong Goes to Net*, WASH. POST, Aug. 7, 1999 at A14.

162. This section will discuss several of these international agreements and the relative protections they afford.

163. As will be discussed below, each of the agreements described in this section, in fact, leaves room for state regulation of expression in the name of protecting the public health and welfare. *See* discussion *infra* Parts III.C.1–III.C.3.

164. *See Regardless of Frontiers, supra* note 30, at A.

165. *See id.*

1. The Universal Declaration of Human Rights

The Universal Declaration of Human Rights ("UDHR"), adopted in 1948 by the United Nations,[166] broadly proclaims freedom of expression for signatory States. Article 19 of the UDHR states: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any medium regardless of frontiers."[167]

Article 12 further provides that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence."[168] Opponents of excessive government regulation of speech on the Internet have pointed to the "through any medium" language to emphasize that the broad standards established by the Declaration were intended to provide protection for new media that signatory nations could not have anticipated at the time the Declaration was adopted.[169]

Despite its broad language, the UDHR recognizes some exceptions to the basic protection of expression it was intended to promote.[170] For example, Article 29(2) provides that the protection of public welfare is a legitimate reason to limit expression.[171] The protections of the UDHR are therefore subordinated to a state's police power to protect "morality, public order, and the general welfare."[172] These categories are vast, however, and their breadth allows a wide range of opinion on what exactly "protection" of "morality" and "public order" would mean. Moreover, the line between protection of morality and impermissible regulation of public opinion is unclear at best,[173] and a genuine question exists as to whether it is at all necessary for a State to control expression in order to protect morality.

Despite the wide recognition of the UDHR internationally, the UDHR is not a treaty and, as such, does not have the force of law.[174] However, over

---

166. Universal Declaration of Human Rights (UDHR), Dec. 10, 1948, G.A. res. 217A (III), U.N. Doc A/810 at 71.

167. *Id.* at art. 19.

168. *Id.*

169. *See Regardless of Frontiers*, *supra* note 30, at A.1.

170. As the text following will explain, the treaty leaves room for control of speech and expression as a function of the state's exercise of its police power.

171. *See* UDHR, *supra* note 166, at art. 29(2).

172. *Id.*

173. Consider the Malaysian example: spreading rumors of rioting arguably undermines public order, but also may play an important role as a political voice. *See* discussion *supra* Part III.B.1.

174. *See Regardless of Frontiers*, *supra* note 30, at A.1.

time the UDHR has become a normative instrument[175] and has created certain limited legal obligations for member states. It has been incorporated by law into the jurisprudence of member nations in two ways. First, evidence of consensus of opinion and practice exists for many member states[176] whose courts and legislatures have broadly incorporated the principles embodied in the UDHR into their own laws.[177] Secondly, the language and ideological thrust of the UDHR has been incorporated into subsequent treaties, some of which are outlined below.[178]

2. International Covenant on Civil and Political Rights

The International Covenant of Civil and Political Rights ("ICCPR") expands upon the principles first established through the UDHR. The ICCPR echoes the UDHR's Article 19 protection of expression, declaring that "[e]veryone shall have the right to hold opinions without interference . . . [and to] freedom of expression."[179] Somewhat more explicitly than the UDHR, the ICCPR extends protection of expression to all forms of media: "[t]his right shall include freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media."[180] Clearly, then, the ICCPR is also aimed at hindering government control over the circulation of "information," a category broad enough to protect expression such as the Internet encourages.[181]

Like UDHR, the ICCPR also recognizes certain limitations on individual expression. Article 19(3) of the ICCPR provides that restrictions on freedom of expression are valid if they are "provided by law and are necessary (a) For respect of the rights or reputation of others; [or] (b) For the protection of national security or of public order, or of public health or morals."[182] Again, while protection of speech in every legal regime has been limited at least by reservation of a police power to the state, the categories of "public order, . . . health or morals" are sufficiently ambiguous to permit significant

175. *See id.*

176. *See id.*

177. *See id.*

178. *See* discussion *infra* Parts III.C.2–II.C.4.

179. United Nations International Covenant on Civil and Political Rights (ICCPR), U.N.T.S. No. 14668, vol. 999, 171, art. 19 (1976).

180. *Id.*

181. *See id.*

182. *Id.*

infringement upon expression that is all to easily deemed "harmful" in some way.

Under the ICCPR, signatory states are required to submit periodical reports demonstrating that they have taken measures to protect and advance certain enumerated human rights, one of which is freedom of expression.[183] A Human Rights Committee reviews these reports, identifies possible violations of the covenant, and recommends solutions through advisory opinions.[184]

Enforcement of the ICCPR is likely to be inconsistent at best.[185] States could easily omit from their reports certain information likely to serve as the basis for a determination by the Committee that rights have been violated. Even private causes of action pursued under the covenant do not bring every violation to the Committee's attention since private remedies must first by exhausted by the party in question.[186] Finally, the greatest obstacle to enforcement of the ICCPR lies in its optional status.[187] The advisory opinions of the Committee, like those of many international bodies, are just that—advisory—and the Committee lacks significant enforcement power.[188]

3. International Covenant on Economic, Social, and Political Rights

The International Covenant on Economic, Social, and Cultural Rights ("ICESCR") echoes the language of the UDHR in recognizing the important "benefits to be derived from the encouragement and development of international contacts and cooperation in the scientific and cultural fields."[189] However, like the UDHR and the ICCPR, the ICESCR establishes only a review system, not an enforcement power, for any expression it protects.[190]

---

183. *See* ICCPR, *supra* note 179, at art. 40, § 1.

184. *See id.* at § 2.

185. *See id.* Advocates of free expression online have noted that the international patchwork of treaties protecting speech leave holes in which national governments could expansively control online speech and expression by way of its police power. *See Regardless of Frontiers, supra* note 30, at A.2. *See also* ICCPR, *supra* note 179.

186. *See* ICCPR, *supra* note 179, at 15–16.

187. *See id.*

188. *See id.* at 15.

189. International Covenant on Economic, Social, and Cultural Rights, 1976 U.N.T.S. No. 14531, vol. 993, 3, art. 15.4.

190. *See id.* at art. 17.1.

4. Adequate Protection for Internet Service Providers Doing Business Overseas?

Despite the strong language of these international accords for the protection of expression, their enforceability is a major limitation.[191] At best, so far the agreements have offered normative ideals, not enforceable standards,[192] and have been effective only insofar as courts and legislatures have taken it upon themselves to incorporate those standards into their national law.[193] Moreover, all of the accords recognize a fairly broad police power on the part of the state to regulate expression considered harmful to members of the community, especially children.[194]

Thus, although these agreements evidence an international impulse to protect a broad range of expression, their usefulness is mitigated by three basic limitations. First, each one of the international agreements contemplates state regulation of expression on the Internet through the exercise of the state's police power.[195] Since there is arguably no logical limit on what types of speech could in some way affect public morality or political opinion, such police power could be exercised expansively. Second, these international agreements do not create vigorous enforcement mechanisms.[196] Third, in practical terms, it is very unlikely that all nations in which ISPs wish to do business, even western democratic ones, will altogether abandon attempts to control the type of expression to which their citizens have access.[197] In short, then, international accords might successfully reduce the risk of unwarranted ISP liability as willing nations incorporate the principles of the agreements into their own national law. But it is unlikely, given the limitations described above, that the agreements themselves could ever establish blanket protections for ISPs facing potential criminal liability for acts taken by third parties over whom ISPs have no control.[198]

---

191. *See generally Regardless of Frontiers*, *supra* note 30, at D.

192. *See id.*

193. *See id.*

194. *See* discussion *supra* Parts III.C.1–III.C.4.

195. All of them, that is, reserve some room for a nation's police power, but do not help define what, in the view of the framers of these documents, is a *legitimate* exercise of that power. *See* discussion *supra* Parts III.C.1–III.C.4.

196. *See id.*

197. The United States itself, for example, attempted a second Internet pornography bill even after the first had fallen to serious constitutional infirmities. *See* 47 U.S.C. § 231 (1999). *See also* discussion *supra* Part III.A.2.

198. This is due to the many enforcement problems elucidated above. *See* discussion *supra*

IV. THE UNIQUE NATURE OF COMMUNICATION ON THE INTERNET AND RESULTING PROBLEMS OF CONTENT CONTROL

Because of the global reach of the Internet,[199] ISPs typically lack control over and notice of illegal material stored on their networks.[200] Again, this lack of notice is not likely to arise from the deliberate failure of ISPs to screen their networks from expression that is illegal in the jurisdictions in which they operate. Rather, the difficulty arises out of the lack of meaningful geographical and jurisdictional boundaries on the Internet that makes such screening impossible.[201]

The content of the Internet is created by users in nearly every part of the globe.[202] An anonymous user in one jurisdiction could post an image to a network based in another jurisdiction, which itself gets Internet access from another, larger service provider in yet another jurisdiction.[203] In any one of these jurisdictions, the image might be illegal, and if so, the temporary storage of the image on the storage device of any of the ISPs could lead to prosecution.

Indeed, this is what happened in the *Somm* case, where some of the images used to form the basis of the charges against Somm were not even stored on the proprietary servers of CompuServe USA, but were merely accessible to German CompuServe users through CompuServe's provision of general Internet access.[204] However, despite the difficulty of convincingly alleging that ISPs themselves have broken the law when they have merely provided access to the Internet itself, nations can and do impose criminal liability on ISPs for certain types of illegal content appearing on their networks.[205]

Moreover, although it is part of a domestic corporation's duty of due diligence to investigate and obey the laws of foreign jurisdictions,[206] the possibility that anonymous users could post illegal material on a network accessible from anywhere in the world makes it nearly impossible that ISPs

---

Parts III.C.1–III.C.4.

199. *See* Harmon, *supra* note 47, at A1.

200. *See* Moritz, *supra* note 2, at B7.

201. *See* Harmon, *supra* note 47, at A1.

202. *See id.*

203. *See Somm*, *supra* note 4, at V.A.

204. *See id.*

205. *See generally* discussion *supra* Parts III.A–III.B.

206. According to the Local Court, Somm had a duty to exercise reasonable diligence in avoiding infractions of the law through CompuServe Germany. *See Somm*, *supra* note 4, at IV.2.A.5.

could know, on a day-to-day basis, the exact content of their networks, illegal or not.[207] There would thus be little opportunity for ISPs to comply with the laws of foreign jurisdictions with respect to restricted content. Given all of the above, transnational service providers face certain predictable difficulties:

> (1) ISPs will not be able to police their own networks to prevent themselves from incurring civil or criminal liability for illegal content;
> (2) Such policing, even if technically feasible, would be too financially burdensome for ISPs to continue to provide Internet access in foreign jurisdictions; and therefore
> (3) Transnational ISPs doing business overseas will be unable to indemnify their officers from criminal and civil liability in foreign jurisdictions in the absence of an international agreement either:
> (i) removing restrictions on content on the Internet;[208] or
> (ii) universally limiting the liability of service providers for the acts of third parties.

Clearly, until these inadequacies in current international law are addressed, transnational ISPs will continue to face uncertainty and possibly even criminal liability for acts taken by parties over whom those ISPs have no control.

V. CONCLUSION

There is a clear need for a multilateral treaty which would establish appropriate protections for ISPs from criminal liability arising from acts taken by third-party users.[209] Only such protections would make it possible for an ISP to do business in a foreign jurisdiction that criminalizes certain forms of expression without itself being unpredictably exposed to criminal liability. Although the excesses of the *Somm* decision were corrected on appeal,[210] the case nonetheless raises the specter of criminal prosecutions in other jurisdictions. Far from remaining the concern only of civil libertarians, the question of ISP liability in a world of differing standards for the protection of speech vitally affects the viability of the Internet as a global

---

207. Such a lack of knowledge did not, of course, prevent the court in *Somm* from finding that the accused intended to distribute the banned content to German CompuServe users. *See Somm*, *supra* note 4, at IV.1.3.b.

208. Such a solution is unlikely at best. *See* discussion *supra* Part III.C.4.

209. No such treaty currently exists. *See* discussion *supra* Part III.

210. *See* Schmertz & Meier, *supra* note 98, at 12.

marketplace without borders. The resolution of this question will help determine the real cost of doing business for the large, transnational ISPs that constitute the bedrock of this marketplace.[211] If the Internet itself is a truly global network, protecting ISPs from undeserved liability will require a global solution.

Mark Konkel

211. "Internet Service Providers have proliferated at a breathtaking pace.... Between mid-1995 and mid-1996, five million servers were created." Oumarou & Lefort, *supra* note 48, at 38.