The "facts" of El Salvador according to objective and new journalism. *Journal of Communication Inquiry*, 13(2), 75-96, 1985.

9

Advantage ISP: Terms of Service as Media Law*

Sandra Braman and Stephanie Lynch

Although in the popular imagination the Internet remains a diffuse cloud, in practical terms those who use e-mail and surf the web do so through the Internet Service Providers (ISPs) through which they gain access (Blumenthal and Clark 1997). As the proportion of our communicative and informational lives conducted on-line steadily grows, the reality of ISPs as determinants of the conditions under which communicative activity takes place is transforming the de facto communication law environment. The abandonment of traditional First Amendment rights and forced transfer of the intellectual property rights of individuals to ISPs so far occur beneath the radar in contracts unread and lawsuits scattered throughout topic-specific analyses.

It has always been the case that any constitutional right—including those of the First Amendment—can be voluntarily yielded by contract. Historically, however, only occasionally were rights were so affected, few or only single rights were thus yielded up, and the contexts in which such a decision was made were those in which it was possible to make a choice among alternatives. In contrast, the contractually generated speech environment of ISPs restricts the rights of almost everyone and requires abandonment of a wide range of rights. As Acceptable Use Policies (AUPs) and Terms of Service (TOSs) increasingly harmonize with each other across ISPs, these restrictions on rights take place in a context in which the vast majority of users cannot choose an alternative.

The number of individuals who have found their speech constrained by ISPs is not known because there are no reporting requirements on ISPs

and not all instances reach the courts, but anecdotal reports in extensive discussions in usenet groups suggests the problem is not infrequent. ISPs are beginning to act on their licenses to the intellectual property rights of content produced by their users in pay-for-access websites to, for example, salacious material garnered from user e-mail and further use of user-created content by ISPs must be expected. Meanwhile complementary elements of the legal environment that support ISPs in such moves are steadily being strengthened and a general climate of acceptance of some of the more fundamental features is being developed through systematic focus on single elements of the overall picture. The end result could well be a wholesale shift in the possibilities of free expression in the United States without public discussion and decision-making on the fundamental constitutional issues at stake. New laws and regulations put in place since 9/11 have significantly increased the responsibility of ISPs to act essentially as agents of the government, enhancing their quasi-regulatory role by adding a range of enforcement activities.

After a brief review of the development of the regulatory aspects of ISPs, this chapter presents the results of a study of ISP rules in place in spring of 2002 that have media law-like effect. Based on a close reading of texts in order to gain the greatest sense of differences in nuance and detail, the group of ISPs studied are largely commercial in nature but does include a range of types so that some comparison between U.S.-based vs. non-U.S.-based and commercial vs. noncommercial could be accomplished, as well as a comparison between ISP rules of today and those of the past. Analysis of the legal or quasi-legal effect of ISPs is important at this stage in their development because of the effects of path dependence on development of the industry and because the history of particular practices is an important element in constitutional analyses of the acceptability of those practices.

Doing so also provides a de facto list of policy issues in the contemporary internet environment that need attention by policy-makers. The chapter concludes with a look at possible responses to this situation.

The Development of ISP Regulatory-Like Functions

Discussion of ISPs as regulators began to appear in 1996 (Johnson and Post 1996; Reidenberg 1996). Since that time several factors encouraging the organizations to fill this function have been identified, but there has

been almost no systematic analysis of the ways in which the function has been filled, effects of exercise of the function, or the constitutional acceptability of the practices.

Analyses of the ISP Regulatory Function

While media and telecommunications law casebooks and textbooks regularly organize their analyses of law and regulation as they pertain to specific media and industries, none of the cyberlaw books to date has yet explicitly treated communications law in the ISP environment (Baumer and Poindexter 2002; Ferrera et al. 2001; Girasa 2002; Lemley, et al. 2000; Lipschultz 2000; Maggs et al. 2001; Rosenoer 1997). The expansion of the ISP role in enforcement of state-made laws and regulations is receiving analysis (Frydman and Rorive 2002; Zittrain 2003), but there have been very few studies of ISP-made "law" in AUPs and TOSs.

One relatively shallow study of 11 common abuses of e-mail that combined acceptable use and general office policies that found attention to such abuses in every agreement and unsurprising differences only in degree of sensitivity to flames and newsgroup hosting problems (more in ISPs than in the other categories) and concern about leisure surfing (more in organization-specific access systems) (Siau et al. 2002). A study of the AUPs of local and state government agencies conducted in 1998 focused on hierarchical decisions regarding the identities of those permitted to access the internet (Menzel 1998). It did, however, yield a useful distinction among types of rhetorical approaches used in AUPs: some merely remind the user that the internet is no different from any other information technology and that the user is therefore subject to the same ethical and legal standards used elsewhere, some offered detailed statements of acceptable and unacceptable behaviors, and some offer general guidelines for internet-specific behavior. A study of the treatment of information security at ISPs concluded that policies alone are ineffective and need to be complemented with ongoing education and training not only of network administrators but also of users (Nosworthy 2000).

Development of the ISP Industry

As an industry, ISPs are still seeking their identity. Their early history was unusual, quickly achieving mass market status, becoming geographically pervasive, and offering a diverse spectrum of services. The nature of the ISP industry is still evolving: Firms in traditional media industries such

as journalism experiment with providing ISP services to support other on-line activities, external entities such as courts have defined ISPs as a subset of telecommunications for purposes of legal analysis, and devoted ISPs continue to explore the economic possibilities of activities such as distributed computing that are utterly new (Greenstein 2000). ISP experimentation is currently underway with various business models and lines of activity, geographic reach and structure, and the role of ISPs vis a vis other approaches to integrating the "network of networks" (Downes and Greenstein 2002; Noam 2001). Meanwhile the ISP industry continues to expand, partially because the technical and financial barriers to entry have dropped and partially because the market has grown so explosively (Phillips 2001; Hallman and McClain 1999). The largest ISPs continue to grow through acquisition of start-ups and smaller entities.

Conditions are still open for experimentation for a variety of reasons: Operating conditions are no longer those of the internet's early "end to end" years in several dimensions of importance from a legal perspective for reasons that, as Blumenthal and Clark (1997) note, include loss of trust, the appearance of more demanding applications, a drop in the sophistication of users, and the desire of ISPs themselves to provide service differentiation. It is not yet clear whether ISPs should be identified as members of the "cyberspace community" more broadly defined, or as the powers that govern that community (Biegel 2001). Meanwhile very few users understand the functions of ISPs (Engel 1999), or the law dealing with them (Townsend et al. 2000).

Distinctions among ISPs

Of course ISPs are not all alike. Various approaches to distinguishing among them have been put forward. Doing so by geographic reach yields two distinctions: between local, national, and international ISPs; and between ISPs serving urban as opposed to rural areas (Greenstein 2000, 2001). Doing so by type of user results in a distinction between businesses and individuals as ISP customers (Engel 1999). Doing so by services offered and/or functions filled (Greenstein 2000) results in distinctions between those that provide basic access, high speed access, and complementary services; or in a finer articulation, between those that provide basic access (up to T-1), frontier access (faster than T-1), networking, hosting, and web page design. Doing so by architecture, placing the posi-

tion of each ISP within the structure of the internet, results in distinguishing between ISPs with the functions of transit backbone, downstream ISPs, online service providers that package content, and firms that specialize in web site hosting (Gorman and Malecki 2000).

Each of these typologies highlights different dimensions of the ways in which ISPs operates as actors in the legal environment and as regulators or quasi-regulators in themselves. The geographic scope of an ISP could have implications for jurisdictional analyses (Bonnett 2001). User distinctions suggest economic implications of the ways in which ISPs intervene in use content and behaviors, but the one study of ISP user satisfaction (Wetzel 2000) did not include legal and quasi-legal elements in its survey. Service distinctions draw attention to the variable degree with which ISP Terms of Service (TOS) or Acceptable Use Policies (AUP) can have constitutional implications. And architectural distinctions such as the nature of the peering structure, the position of an ISP within the internet writ large, and innovation in technologies such as routers have implications both for interactions among regulatory approaches across ISPs and for the types of regulatory tools that are available to ISPs (Besen 2001).

Factors Stimulating the ISP Regulatory Function

To be generous, ISPs have come to fill the legal space as a consequence of their roles as what Greenstein (2001) describes as "technological mediators," providing necessary adaptations between a changing technical frontier and unique user needs. Many of the regulatory restrictions are the result of limits to bandwidth or, conversely, responses to the cost of expanding bandwidth. Even though ISP responses to these features of their situation are understandable, however, they do not make them constitutionally—or socially—acceptable. While these practices may be defended as responsible management, they often cross the line into manipulative control of content and applications of types long rejected in the larger communicative world. Some may argue that ISPs should be accepted as governance mechanisms, but they meet neither the regulatory criterion of being all-encompassing, (Biegel 2001) nor have they been developed in a democratic manner.

AUPs and TOSs have become more detailed and elaborate over time, stimulated by several factors. Doing so in many cases would be among the functions they serve their customers as technological mediators. In

some cases they are responding to pressure from at least some of their users. intervention in network content and behaviors may be a natural outgrowth of the detailed, consistent, and regular monitoring of online activity carried out by network administrators. Ever-greater numbers of technical methods of intervention continue to appear. So do tools for enforcement, which now include slowing response time for a service an ISP wants to discourage, channeling surfers through advertisements it wants them to see, and identifying patterns of behavior that monitors can watch based on profiles (Lessig 1999). Tools that can be used by ISPs for governance include rules announced to members, stigmatizing behaviors as a way of triggering community norms to help regulate, manipulation of prices (increase, taxation of particular uses, or differential prices depending on user), changes in architecture, and monitoring of behaviors.

ISPs are also responding to developments within the law. Laws dealing with ISPs continue to grant ever-greater freedom to operate without fear or liability, (Patel 2002) while legislation has so far been unable to satisfactorily curb unwelcome on-line behaviors. Three types of liability regimes have been applied to ISPs:

(1) A negligence regime was first adopted in the United States and is presently employed in Europe that holds ISPs liable when they fail to exercise due care in monitoring of third party content.

(2) A strict liability regime was experimented with in both the U.S. and in Europe that holds ISPs liable for all injuries resulting from third party content.

(3) A no liability or conditional liability regime is presently used in the United States that holds ISPs almost completely immune from liability for third party content, conditioned only on minimal responsibilities as outlined in Sec. 230 of the Communications Decency Act (Schruers 2002).

User Responses

While theoretically any ISP can say to a user that s/he can "walk with one's fingers" to another ISP if there is dissatisfaction with the terms under which one may use the ISP, in reality several factors make this less and less practicable: First, terms of Service and Acceptable Use policies are increasingly becoming standardized so that there is less and less difference across ISPs; thus in most cases there is nowhere meaningfully different to go. Second, those ISPs that offer the greatest geographic scope

tend to be those that are most restrictive—meaning that those who are most actively involved in public life beyond the local community level are those whose rights will be most restricted. The trend of mergers and acquisitions in the ISP industry exacerbates the first two factors.

Users and user groups are not without tools for response. A number of usenet groups provide venues for discussion of dissatisfactions with ISPs, though such conversations often tend toward discussion of the personalities of network administrators rather than the rule structure itself. Standards that reputable ISPs should meet are beginning to be discussed, though until now these have had to do with technical aspects of service rather than regulation of service. Those who bundle individual users into groups, such as managers of wired office or apartment buildings, are being provided with recommended terms of service, though again the only inclusion pertinent to quasi-legal interventions by ISPs is emphasis upon the nonexclusive license rights that make it possible for users to choose other ISPs if they are unhappy (Puentes and Rothenberg 2001). A consumer movement that joins together individuals concerned about threats to civil liberties presented by ISPs is beginning to appear (Akdeniz 2000). ISP management of communication content and behaviors receives a significant amount of discussion in usenet groups, though this discussion rarely moves into action. Some communication policy advocacy groups do things such as monitor websites that are blocked by filtering software. The most effective responses to date, however, appear to be individual- (Kevlin 2001) or ISP-level (Biegel 2001) use of technical methods for blocking content deemed inappropriate, though this has proven effective so far only for spam with the Realtime Blackhole List.

Methodology

This study examined a relatively small number of cases in depth for maximum detail and nuance. While Greenstein grouped together a number of different approaches to the same problem in order to facilitate computerized content analysis of thousands of user agreements, this study employed close reading of texts in order to discern differences in stance presented by different ways of wording restrictions on restricted content and activities that are important from a legal perspective.

The study examined AUPs and TOSs of ISPs as they existed during the

spring of 2002.[1] ISPs varied by geographic locus and reach, size, target market, and commercial nature. The study included the largest commercial ISPs as ranked by size, plus a small ISP from each region of the U.S. and an ISP from each of the other continents besides North America. "ISP" was defined for the purposes of this study as an institution that provides an ISP-like experience for the user. Thus examples of access to the web through K–12 schools, universities, and public libraries were included in the sample. A list of the ISPs studied can be found in table 9.1.

The result was identification of 59 rules that pertained to ISP-user relations (see table 9.2), divided into those dealing with general matters (about policies themselves, service limits, and limits to account use), identity, user liability, lack of ISP liability, and ISP treatment of privacy; 42 rules dealing with content (see table 9.3), divided into those dealing with illegal content, intellectual property, and other content restrictions; and 38 rules dealing with behavior (see table 9.4), divided into those dealing with illegal behavior, security, user treatment of privacy, and other behavior restrictions. The percentage of total ISPs with each of the specific rules identified can be found in tables 9.2, 9.3, and 9.4, along with a breakdown of commercial vs. noncommercial ISP rules.

While the original intent of the study was to compare the earliest versions of these agreements with their contemporary versions, only half a dozen of the earlier agreements were available through use of the Wayback Machine as others were not on-line but incorporated into software licenses off-line. These did provide an opportunity to make a first pass at examining the development of AUPs and TOSs across time.

Interpretations of user knowledge and responses were acquired via a review of the literature and through analysis of discussion of the regulatory practices of ISPs in usenet groups archived by Google located through use of search terms such as ISP, lawsuit, AUP, TOS, and privacy policy and from a sampling of messages in the news.admin.net-abuse groups that are dedicated to internet abuse issues.

Discussion

The relationship between users and ISPs as defined by AUPs and TOSs is best described currently as "advantage ISP" for a number of reasons described here in generalized form and discussed in more detail below. It

is worth noting that while some of the rules—those dealing with infringement of intellectual property rights, invasions of privacy, and content and behavior so labeled—deal with matters treated as illegal under the laws of the United States, most forbid activities that are legal under U.S. law. In addition to the areas discussed in detail within the paper, the charts provide detail on rules put in place to protect personal privacy, encourage respect for intellectual property rights on the part of users, protect network security, and explicitly forbid content and behaviors already illegal under U.S. law.

- *Knowledge*: Users know little about rules or enforcement tools, practices, and history.
- *Liability*: Users are liable for the consequences of their uses of the ISP—whether or not intended—while ISP's have almost no liability even for failures of service for which telecommunications carriers were traditionally liable.
- *Intellectual property rights*: Users are forced to license all content to ISPs, and often publicity rights as well.
- *Abandonment of ponstitutional protections:* Agreements drafted by ISPs abandon constitutional standards for restrictions on speech of narrow tailoring, establishment of criteria to be met before restrictions can be deemed acceptable, and avoidance of vagueness and overbreadth, resulting in creation of a speech environment significantly more restrictive than that developed for society at large through judicial analysis of the aspects of constitutional law that deal with information, communication, and culture.
- *Comparative analyses:*
  (1) Commercial vs. noncommercial: Noncommercial ISPs provide greater protections for free speech and the intellectual property rights of users, but less in the way of privacy protections.
  (2) Current vs. past: The numbers of rules constraining communicative content and behaviors by ISPs is constantly growing. Some rules are dropped over time, but no pattern was discernible in this area
  (3) U.S.-based vs. non-U.S.-based: Non-U.S.-based ISPs provided less detail in the areas of intellectual property rights and privacy, but tended to restrict more areas of content and behavior that are legal in the United States and did not allow anonymity.

Knowledge

ISPs have the advantage in terms of knowledge about regulatory rules and practices in several ways.

Table 1
ISPs

AOL	By far the largest national ISP, with more than 26 million subscribers and 17.5% of market share. Offers TOS and privacy policies on its website, but maintains separate policies for subscribers to the service. Access to these appears to be limited to subscribers and requires the AOL software to access.
APCi	Provides internet access in the midwest United States, focusing on the St. Louis metro area.
AT&T	Dial-up service is ranked #10, with 1.4 million subscribers.
AT&T 1997	AT&T's policy as of June 6, 1997.
Bellsouth	Regional (Southeast) ISP offered through Bellsouth telephone company; ranked 15th with 730,000 subscribers.
Cablevision	Cable company providing national high-speed internet access; ranked 17th with 560,000 subscribers.
Charter	Communications company offering high-speed cable modem access. Ranked 14th, with 645,000 subscribers.
Chicago Public Schools	Chicago Public Schools
Columbia University	Columbia University
Compuserve	Owned by AOL, but operates separately. Ranked 6th, with 3,000,000 subscribers.
Earthlink	Offers various services (dial-up, broadband, etc.), each with its own policy. Only dial-up analyzed. Earthlink dial-up ranked 4th, with 4,800,000 subscribers.
Earthlink 2000	Earthlink's policy as of March 2 and 11, 2000
GOL-Japan	Provider based in Japan. GOL: Global OnLine.
Inter.net	Global provider, looked at Canadian branch.
Juno	Merged with NetZero to form United Online, but still maintains its own service. Merged company ranks 3rd and has 5,600,000 subscribers.

Juno 2000	Juno's policy as of March 1, 2000
Mindspring	Has been bought by Earthlink.
MSN	AOL's closest competitor, but still lags behind. Ranked 2nd, with 8,000,000 subscribers.
MSN 1996	MSN's policy as of October 26, 1996
M-Web	South Africa-based provider.
Naperville Public Library	Naperville Public Library
Pacific Internet	Singapore-based ISP.
Panix	Oldest commercial internet provider in New York.
Prodigy	Dial-up service ranked 5th, with 3,600,000 subscribers.
Prodigy 1999	Prodigy's policies as of April 22, 1999.
Rain	"Public Internet Broadcasting" service based in California.
San Francisco Public Library	San Francisco Public Library
Simplecom	West Alabama ISP.
Simplecom 1999	Simplecom's policy as of April 20, 1999.
Tuscaloosa City Schools	Tuscaloosa City Schools
University of Texas	University of Texas
Verizon	Communications company offering internet access among other services. DSL is ranked 11th, with 1,200,000 subscribers.
Worldcom	Commercial internet provider

Table 9.2
ISP-User Relations

	All (N=27)%	Com (N=21)%	NonCom (N=6)%
General			
Policies			
Rules in one place	55.56	42.86	100.00
Policy change alert	40.74	52.38	—
Where policy applies	37.04	42.86	16.67
Dispute res. process	29.63	33.33	16.67
May change ISP software	11.11	14.29	—
Member audit org.	11.11	14.29	—
Copyright infringement report process	22.22	28.57	—
Service limits			
Message retention	18.52	23.81	—
Disk space	25.93	28.57	16.67
On-line time	44.44	57.14	—
Website traffic	37.04	38.10	33.33
Number of sessions	07.41	09.52	—
No multiple logins	37.04	47.62	—
Limits to account use			
No unauthorized access	66.67	71.43	50.00
No use of other's acct	51.85	52.38	50.00
May not resell service	40.74	52.38	—
Pay for all transactions	11.11	14.29	—
Identity			
Anonymity allowed	11.11	14.29	—
No anonymity allowed*	—	—	—
No false ID	18.52	19.05	16.67
No false ID to mislead	14.81	19.05	—
No forging of headers	48.15	61.90	—
No impersonation	40.74	47.62	16.67
No use of vulgarity in screen names	07.41	09.52	—
User Liability			
ISP can remove material of concern	48.15	61.90	—
ISP indemnified against damage to user	48.15	57.14	16.67
User liable for account	40.74	47.62	16.67
User liable for damage to ISP	18.52	23.81	—

*Included in older AUPs

Table 9.2
(continued)

	All (N=27)%	Com (N=21)%	NonCom (N=6)%
No ISP Liability			
Accidental deletion/failure to store messages	25.93	33.33	—
Content/links	59.26	71.43	16.67
Copyright infringement by users	29.63	28.57	33.33
Transmission errors	37.04	47.62	—
Damage from material received	51.85	61.90	16.67
Damage from transactions	22.22	28.57	—
Failure/delay in removal of material	14.81	19.05	—
Interruption	44.44	57.14	—
Lack of timeliness	29.63	33.33	16.67
Loss due to unauthorized account use	14.81	19.05	—
Security lapse	33.33	42.86	—
Viruses, worms, etc	33.33	33.33	33.33
Privacy (ISP)			
Data collection techniques			
Cookies	25.93	33.33	—
Request info from user	29.63	38.10	—
User must update info	25.93	33.33	—
Other collection techniques	14.81	19.05	—
Stat techniques described	29.63	38.10	—
Types of info collected			
Personal information	37.04	47.62	—
Advertising presented	18.52	23.81	—
Computer	25.93	33.33	—
Computer use	22.22	28.57	—
Software	07.41	09.52	—
Use of information collected			
By function	37.04	47.62	—
No sale of personal info	22.22	28.57	—
Data sharing partners	40.74	52.38	—
Will cooperate with govt.	51.85	61.90	16.67
User options			
General opt-out	25.93	33.33	—
Directory listing opt-out	03.70	04.76	—
Detailed consent to uses	14.81	19.05	—
Other opt-out	03.70	04.76	—
Correction possible	29.63	38.10	—

Table 9.3
Content

	All (N=27)%	Com (N=21)%	NonCom (N=6)%
Illegal content			
No unlawful content	25.93	33.33	—
No defamation/libel/slander	44.44	57.14	—
No incitement to violence	11.11	09.52	16.67
No obscenity	62.96	66.67	50.00
Intellectual property (IP)			
IP rights claimed by ISP			
ISP has license to all postings	11.11	14.29	—
ISP has license to all postings to gen. public	25.93	33.33	—
May sub-license postings	07.41	09.52	—
May use postings for commercial purposes	11.11	14.29	—
May distribute postings	29.63	38.10	—
May produce derivative works	25.93	33.33	—
May publicly perform/ display postings	22.22	28.57	—
May reproduce postings	22.22	28.57	—
May use user's name in connection with postings	07.41	09.52	—
May delete submission	22.22	28.57	—
No compensation for use of material	07.41	09.52	—
IP rights infringement by user			
May not violate copyright	74.07	76.19	66.67
Download only one copy	03.70	04.76	—
May not create derivative works	22.22	28.57	—
May not delete/alter attribution	25.93	28.57	16.67
May not download w/o rights	40.74	38.10	50.00
May not post/upload w/o rights	62.96	71.43	33.33
May not reproduce other than for personal use	29.63	33.33	16.67

Table 9.3
(continued)

	All (N=27)%	Com (N=21)%	NonCom (N=6)%
Other content restrictions			
On non-personal objectionable content			
No inappropriate content	14.81	19.05	—
Use filters	03.70	04.76	—
No indecency/pornography	37.04	42.86	16.67
No material violating internet norms	14.81	19.05	—
No objectionable content	11.11	14.29	—
No posting off-topic (newsgroups)	44.44	57.14	—
No profanity	18.52	23.81	—
On personal abuse			
No harmful content	22.22	23.81	16.67
No abuse of others	33.33	42.86	—
No contesting crimes against humanity	03.70	04.76	—
No hate	37.04	42.86	16.67
No flaming (newsgroups)	11.11	14.29	—
No threat to person/ property	66.67	85.71	—
On promotional efforts			
No chain letters	55.56	57.14	50.00
No charity requests	03.70	04.76	—
No contests	07.41	09.52	—
No petitions	03.70	04.76	—
No pyramid schemes	44.44	57.14	—
No spam	51.85	66.67	—
No surveys	07.41	09.52	—

Table 9.4
Behavior

	All (N=27)%	Com (N=21)%	NonCom (N=6)%
Illegal behavior			
No use for unlawful purposes	88.89	95.24	66.67
No fraud	18.52	23.81	—
No harassment	70.37	66.67	83.33
No stalking	14.81	19.05	—
Security			
General			
May not cause damage	29.63	23.81	50.00
May not intentionally cause damage	22.22	23.81	16.67
May not compromise security	70.37	76.19	50.00
Methods			
Use anti-virus software	03.70	—	16.67
No cancelbots	14.81	19.05	—
No trojan horses	22.22	28.57	—
No time bombs	03.70	04.76	—
No unauth use of third-party server	33.33	38.10	16.67
No viruses	44.44	52.38	16.67
No worms	25.93	33.33	—
No dist corrupted files	07.41	09.52	—
No dist tools for damaging security	25.93	28.57	16.67
Subject of damage			
Other user	29.63	38.10	—
Site	25.93	28.57	16.67
System	40.74	42.86	33.33

Table 9.4
(continued)

	All (N=27)%	Com (N=21)%	NonCom (N=6)%
Privacy (users)			
General			
No invasion of privacy	33.33	33.33	33.33
Maintain confidentiality	37.04	33.33	50.00
Care in dist personal info	18.52	14.29	33.33
Specific			
No coll of personal info	22.22	28.57	—
No receipt of passwords	11.11	14.29	—
No solicitation of passwords	25.93	33.33	—
No coll of email addresses	11.11	14.29	—
No coll of screen names	07.41	09.52	—
No coll of info re minors	07.41	09.52	—
Other behavior restrictions			
Limit cross-posting	51.85	61.90	16.67
No advertising	37.04	42.86	16.67
No automated queries	03.70	04.76	—
No commercial use	51.85	52.38	50.00
No gambling	03.70	—	16.67
No mail bombs	37.04	42.86	16.67
No mass mailing	40.74	47.62	16.67
No meta-searching site	03.70	04.76	—
No pinging	07.41	09.52	—
No restriction of use by others	62.96	71.43	33.33
No surveys	07.41	09.52	—

Knowledge of Rules While all of the noncommercial ISPs made it easy for users to become aware of the pertinent rules by publishing them all in one place, only approximately 43 percent of the commercial ISPs did so, otherwise requiring users to roam the site many clicks deep in order to gain all the knowledge needed. Just over half of the ISPs studied (all commercial) make clear that they will alert users to any changes in policy; otherwise users must continually check AUPs and TOSs to learn if there has been any change in policy. Some ISPs (11.10 percent) explicitly say they are free to change the ISP software at will and without alerting users to these changes; others may do the same but say nothing on this point. With many different kinds of activities taking place via ISPs, only just over a third indicate to users where specific types of policies apply.

Criteria for Decision-making While rules may be published, the criteria by which those rules are interpreted are not. All explication of administrative procedure, however—whether via the Administrative Procedures Act, regulation, or internal organizational rules and procedures—includes explicit and detailed discussion of the criteria of judgment used. Without making such decision-making rules clear, administrators can act arbitrarily and affected users have no grounds upon which to grieve or petition.

Regulatory Tools A wide range of regulatory-like tools is available to and used by ISPs while most users have neither knowledge of the ways in which those tools are used nor of ISP functions. Often modes of manipulation of content are not known or understood by nontechnical users of ISPs and so they may not be obvious—service may be slowed down, differential pricing may be established, or use habits monitored for development of profiles that can be used to justify further regulatory-like interventions. Means by which information is being gathered about users often are not understood by the users (e.g., clear gif., etc., let alone cookies). Noncommercial ISPs say almost nothing about their data collection practices.[2]

Enforcement Practices While rules are published, the range of possible ISP responses to infringements of rules are not. There is usually some threat of loss of service, but techniques of enforcement short of that and the steps through which decisions about loss of service are implemented and may be grieved are not detailed. Users do not know, for example, if

they will be warned about behaviors they consider normal and acceptable but that are deemed unacceptable by the ISP before service is cut, or not. No means is provided for discussing the acceptability of various practices with the ISP. And in most cases there is no means by which ISP users can communicate with each other about petitioning the ISP for changes of rules felt to be unreasonable.

Enforcement History Unless there is conversation about it on usenet groups or other lists, there is also no public record of restrictions on speech. The importance of public knowledge about enforcement of law and regulation underlies the constitutional principle of public access to trials. Concern over loss of such knowledge is key among the issues raised by privatization of the law; by the 1980s, for example, newspaper companies began to examine their loss of access to records of decision-making of importance to the general public because of its impact as a result of the movement of corporate conflict resolution from the courts to modes of alternative dispute resolution. There is no systematic way of learning how ISP users are actually being treated in the broad areas included in AUPs and TOSs other than through anecdotal discussion on specialized bulletin boards of those cases that make it to the eye of others. Such knowledge is of course critical should user groups desire to seek a change in the rules under which they are permitted to communicate.

Liability

Today a "no," or "conditional," liability regime governs ISPs. For other media, *control = liability*, but ISPs effectively have *control without liability*. Of course neither control nor liability is a binary condition, but across media increases in control have meant an increase in liability. In the area of broadcasting, for example, not only has liability for matters such as libel long accompanied editorial control, but in recent years courts are increasingly insisting that broadcasters are liable for damage wrought by viewers inspired by or imitative of behaviors presented in television programming. While ISPs have pursued legal treatment as information distributors rather than content providers, the courts have not been consistent in this regard (Patel 2002).

Even more importantly, ISPs have insisted upon this identity while simultaneously claiming control over the intellectual property rights over material transmitted via their services through mandatory licensing. Thus

there is a deep contradiction in ISP claims, on one hand, *not* to be content providers and, on the other, that they control all content. This contradiction has not yet received analysis in the courts because liability issues have been treated distinctly from intellectual property issues, but inclusion of the latter in analyses of the former should be expected in coming years. For the moment, however, ISPs have control without liability.

ISPs are not even held liable for service failures of the types for which more traditional types of telecommunications service providers are held accountable, such as interruption of service, security lapses, lack of timeliness of delivery of services, etc. They are able to escape such responsibilities because they are not classified as telecommunications companies. As organizations either new altogether or new to the telecommunications business, they do not have internal histories of concern about service provision. And because their relationships with the transmission network itself are varied but most often not that of ownership, it can be difficult to determine just who should be liable for failures of service. This issue is not likely to be resolved unless and until users demand greater commitments to reliability.

Users, however, are generally held accountable for any type of consequence of their uses of ISP services, whether to another user, a website, or the ISP itself. Importantly, many ISPs do not distinguish between causing damage intentionally and doing so unintentionally. (As we know, it may be possible to unwittingly cause technical damage either through ignorance regarding the technologies involved or through software applications so complex that they cannot be predicted.) The question of intentionality is of particular importance from a legal perspective, for intentionality is always key in constitutional analysis. Explorations of whether or not political speech constitutes clear and present danger, for example, includes the important criterion of intentionality, as does determination of fault in libel suits. Differences between ISP rules and constitutional law on this point mean that an ISP user accused of libel might be found innocent because of lack of intentionality by the courts but still lose service because under ISP rules that criterion is irrelevant.

Anonymity is one way of trying to avoid liability for communications that has been constitutionally protected in the United States because “liability” can translate into “punishment” for dissenting political speech or for corporate whistle-blowers even though both types of content have

great social importance. ISPs have experimented with forbidding anonymity; those that explicitly permit it do so only in those environments in which it has been specifically described as acceptable such as in usenet groups or on lists that include permission for anonymity among their internal rules.

Property Rights

Users of some commercial ISPs are forced to grant the services licenses to all content uploaded or posted, with a slightly larger percentage insisting upon the same license only for content presented to the general public. Where they exist, ISP licenses include the entire bundle of intellectual property rights, with AUPs and TOSs specifying the various rights individually—reproduction, distribution, production of derivative works, performance, and display. While such licenses implicitly include the right of ISPs to make money from user content, two ISPs said they have the right to commercial use of what is posted, one emphasized that it would do so without compensation to the content producer user, and one further insisted on the right to offer further sub-licenses to others for commercial use. One ISP also included the right to use of the name of the person who originally posted or uploaded content, one element of the right to publicity.[3]

Interestingly, despite the protection from liability offered by the Digital Millennium Copyright Act (DMCA) if all of its terms are adhered to, (Wernick 2001) about three-quarters of ISPs in the study did *not* provide information regarding how to report alleged or suspected copyright violations to the organization.

Because ISPs strongly emphasize user adherence to copyright law, an asymmetry in potentials for use is created: ISPs, for example, are free to create derivative works based on content uploaded or posted by users, but users themselves are forbidden to do so.

Abandonment of Constitutional Protections

ISPs forbid many forms of constitutionally protected content both nonpersonal and personal in kind, though two of the ISPs in this study (APCi and BellSouth) insist that despite their rules they are not trying to censor or constrain the free flow of information.

In the area of nonpersonal content over 40 percent of commercial ISPs

forbid posting off-topic, a third prohibit even those kinds of indecency and pornography that do not cross the legal line into constitutionally restrictable obscenity, and almost 20 percent forbid constitutionally acceptable profanity. Similarly, a number of communicative activities that are constitutionally protected, such as conducting surveys, requesting donations for charity, running contests, distributing chain letters, or circulating petitions, are forbidden by some ISPs. Though junk mail is not illegal when transmitted via the Post Office, over half of the ISPs surveyed treated spam as unacceptable. While impersonation and forgery are illegal under any conditions, many ISPs also forbid identity experimentation in screen IDs or message headers (as opposed to message content), even though such experimentation is one of the most noted features of internet use.

Several ISPs used very general terms to describe unacceptable nonpersonal content such as "inappropriate," "objectionable," or "material violating internet norms;" general prohibitions on more personal content included terms such as "harmful" and "flaming." Though hate speech unlinked to action is *not* illegal in the U.S. context, over a third of ISPs placed it on the unacceptable list, and one ISP specifically forbade "contesting crimes against humanity." Laws and regulations can be declared unconstitutional for vagueness (language so unclear that reasonable adults cannot agree on their meaning) and overbreadth (language that may be directed at specific types of unacceptable behavior or content but that is cast in terms so broad that many types of acceptable behavior or content are also included) of the kind exhibited by these types of general terms in AUPs and TOSs, particularly because no criteria are offered for determining when the bar had been crossed.

Behavioral limits on otherwise constitutional activities include restrictions on mass mailings (over 40 percent) and cross-posting of messages to more than one news group (almost 52 percent). A few ISPs forbade use of techniques such as automation of queries, meta-searching websites, or pinging. Because many ISPs distinguish between rates offered personal and business users, over a third forbid advertising and over half forbid use of the ISP for commercial use. Restrictions put in place by some of the ISPs presumably out of a good will effort to protect personal privacy are impracticable at best and offensive at worst, such as forbidding the collection of e-mail addresses, collection of screen names, and collection of

e-mail addresses. Only one ISP, on the other hand, forbade collection of information about minors.

It is legal to restrict constitutional rights by contract, but by function ISPs serve as public fora. Contractual yielding of constitutional rights has historically been limited for two reasons, neither of which applies to the ISP context. Contracts have been undertaken only by individuals or small classes of people, while ISP agreements affect essentially all U.S. citizens. And contracts have previously been entered into only in situations in which doing so is a choice among alternatives—one can choose to take a particular job or not, for example. As ISP AUPs and TOSs become standardized, however, contractual abandonment of one's constitutional rights is taking place in a situation in which there are in fact no alternatives if one wants to communicate or receive information at all electronically. These differences between the use of contracts in other situations in which constitutional rights become limited and their use in the ISP environment suggests that contracts should be abandoned in favor of subjecting ISPs to public forum analysis.

Comparative Analyses

The inclusion of a range of types of ISPs in the study makes it possible to offer comparisons between different categories of ISPs, though the small numbers of each make the comments below only suggestive. Descriptions of the ISPs included in the study found in table 9.1 include detail about the comparative dimensions.

Commercial vs. Noncommercial Commercial ISPs tend to have many more rules than do noncommercial ISPs across categories. Most notably, none of the noncommercial ISPs in this study claimed a license to the intellectual property rights of content posted or uploaded. They also said far less about restrictions on content and behaviors. Noncommercial ISPs also, however, provided much less information about the kinds of data collected about users and ways in which that data is used and did not offer opt-out options for users concerned about protecting their privacy. The conclusion is that users appear to have greater protections for freedom of speech and much less fear about loss of their intellectual property rights when they use noncommercial ISPs, but in turn they may need to be more concerned about protections for their right to privacy.

Present vs. Past Though the original intent of the study was to compare original and contemporary AUPs and TOSs of every ISP in the study, it turned out that only six of sets of earlier agreements were accessible via the tool of The Wayback Machine, and these were not necessarily the first agreements used by each (MSN, 1996; AT&T, 1997; Prodigy, 1999; Simplecom, 1999; Juno, 2000; Earthlink, 2000). The most dramatic finding of the comparison was the explosion in the number of rules: while the average number of rules in the earlier agreements was 29, in spring of 2002 it was 60. Some earlier rules were dropped in current versions of AUPs and TOSs, but there was no discernible pattern in what disappeared. Possible explanations for changes in the terms of agreements over time include changes in ownership, legal impact, experience, and the desire to model examples set by other ISPs.

U.S.-based vs. Non-U.S.-based Four of the ISPs studied were based outside of the U.S. Of course non-U.S.-based ISPs did not include information on where to report infringements of U.S. copyright law. While one of the four did claim a license to all material posted, it did not detail the different elements of copyright as found in U.S. law; there was less concern about copyright infringement by users. There was not as much detail in non-U.S.-based ISPs in the area of privacy. Probably reflecting data privacy rules of the OECD, however, a larger percentage of non-U.S.-based ISPs did provide information about those with whom ISP user data collected would be shared. It is not surprising that non-U.S.-based ISPs included more restrictions on content and behaviors that are legal in the United States but often not elsewhere in the world. Anonymity was not allowed by non-U.S.-based ISPs.

Responses to ISP Regulation

Both economic and legal tools are available to those concerned about these trends in the development of a regulatory-like function for ISPs.

Economic Tools

Both general (consumer movement) and more specific (user group) techniques are available to users who are concerned about these trends, while entrepreneurs may choose to interpret such trends as a means of identifying a market niche.

Consumer Movements Consumer movements, now nascent, can serve several functions: they can educate consumers about issues, stimulate formation of groups large enough to have negotiation heft, and bring issues of concern into public discourse.

User Groups An economic tool of some potential strength is available to users who form into large groups of users. The example has been set by large office and apartment buildings that contract with specific ISPs to provide service to their tenants; while these agreements have tended to focus on reliability of service and marketing restrictions, they could be expanded to include negotiation over the conditions of communications. If all libraries in the American Library Association (ALA), all universities involved in EDUCAUSE, or all schools in a state or a school district, required certain features in their TOS or AUP as terms of a group contract the economics of the situation would force ISPs interested in the business to give up on unacceptable restrictions.

Market Niche On the entrepreneurial side, there is an as-yet-unfilled market niche for the ISP or ISPs that should choose to provide the widest possible protections for freedom of speech and other communicative, informational, and cultural rights as their distinguishing features. Two "public interest" ISPs were included in the study: Panix, which targets political activists in its marketing efforts, and Rain, which explicitly defines for itself a public service role. It is worth noting that while these two do forbid illegal manipulations of identity, they are more open to types of identity experimentation that would be considered legal under other circumstances; they do not insist upon a license to content posted or uploaded; they are more open than many ISPs to use of techniques such as meta-searching; and they have markedly fewer restrictions on content than other ISPs.

Legal Tools

The distinction between voluntary and involuntary communications is a legal tool that may be valuable in the court context, public forum analysis should be of value both in the courts and in Congress, and it is the responsibility of Congress to address violations of and potential changes to copyright law.

Voluntary vs. Involuntary Constitutional law has always distinguished between those situations in which one's speech conditions were voluntary and those in which they were involuntary, with much higher barriers to unacceptable speech in those conditions in which individuals cannot choose to avoid the communications or communicate through another means. The involuntary nature of the need to rely upon an ISP in order to communicate via the net provides an opening for legal analysis of restrictions on speech along the dimension of voluntariness.

Public Forum Analysis The distinction between public and private forums is used by the courts as a first question in determining when restrictions on speech are constitutional. Four types of forums have been distinguished: *Public forums* are publicly owned and controlled, with public functions and history (e.g., parks and sidewalks); restrictions on speech in public forums are subjected to the highest level of scrutiny. *Quasi-public forums* are publicly owned and controlled but are devoted to specific functions and have a history of restricted use (e.g., public universities and military bases); restrictions on speech in such contexts are justified if the speech in question would interfere with the functions to which the venues are devoted. *Quasi-private forums* are privately owned and controlled but serve public functions and have a history of public use (e.g., company towns, shopping malls, and airports); restrictions on speech in these venues are also acceptable if the speech in question would interfere with the functions to which the forums are devoted. *Private forums* are privately owned and controlled, serving private functions and with a history of private use (e.g., homes, personal offices); rules for speech in private forums are up to the discretion of those who own and control them.

Within this typology, ISPs should be considered quasi-private fora: Ownership and control may be public or private, but their functions are primarily public. Since expansion of the internet beyond the original research scientist users, the history of use is primarily public—but because that history is still being formed, bringing public forum analysis into evaluation of ISP acquisition of regulatory-like functions is particularly important right now. The concept of ISPs as quasi-public fora failed in the courts in the courts in cases in which users the concept was used as a defense for the practice of disseminating spam (*America OnLine v Cyber*

Promotions, 1996; *CompuServe v Cyber Promotions*, 1997). The harmonization of ISP Terms of Service and Acceptable Use Policies since that time, however, alters the facts sufficiently that this line of argument would be much more likely to succeed under contemporary conditions.

Copyright Law Mandatory licensing of the intellectual property rights of everyone who communicates via the internet is a de facto change in copyright law that should not have been permitted without explicit policy-making attention. The constitutionality of such a move under current conditions is a matter for the courts, and the question of whether or not such a move should be permitted should be directly addressed by Congress as a matter of statutory law. Neither of these legal processes need wait until ISPs begin taking advantage of the vast quantities of content over which they are asserting the right of commercial use.

Conclusions

This study of the kinds of rules being put in place to constrain communicative content and behaviors on the internet via user contracts with ISPs suggests that without public discussion and largely without public awareness a significant shift is taking place in the actual nature of the increasingly dominant electronic speech environment. There is a long history of carefully crafting constitutional law in such ways that when other social needs must be balanced against speech rights this is accomplished in ways that are as narrowly tailored as possible, specific to the end desired and effective in reaching that end, uses language that is clear and unambiguous, always tries to maximize the opening of alternative venues for speech, and respects the intellectual property rights of those who create content. ISP contracts appear to be ignoring that history and are putting place rules that restrict speech that are broad, vague, and ambiguous; specifically prohibit forms of speech that have been explicitly and repeatedly protected under U.S. law; exhibits no respect for the intellectual property rights of content creators; and does so in an environment in which increasingly there are no alternative venues for speech. Addressing these trends at this relatively early point in the history of use of the internet is critically important to ensure that all of the constitutional effort will not have been in vain. Tracking the development of a

much larger number of ISP Acceptable Use Policies and Terms of Service agreements would be valuable as a means of determining whether or not such efforts are successful.

Notes

1. These agreements appear to change relatively quickly, and since the time of the study some of the smaller ISPs have already changed ownership.

2. The one exception is the mention by one noncommercial ISP of its compliance with Patriot Act requirements regarding surveillance of e-mail and web surfing practices.

3. While intellectual property rights provide a bundle of ownership rights to content produced, the right to publicity—which does not exist at the federal level in the United States but does in about half of the states—provides ownership rights in features of the individual such as the name, likeness, voice, and other identifying characteristics that may have commercial value.

References

Akdeniz, Y. 2000. "New Privacy Concerns: ISPs, Crime Prevention and Consumers' Rights," *International Review of Law, Computers & Technology* 14, no. 1:55–62.

America Online, Inc. v CyberPromotions, Inc., 948 F.Supp. 436 (E. D. Penn. 1996).

Baumer, D., and J. C. Poindexter. 2002. *Cyberlaw and E-commerce*. Boston: McGraw-Hill/Irwin.

Besen, S. 2001. "Advances in Routing Technologies and Internet Peering Agreements," *American Economic Review* 91, no. 2:292–297.

Biegel, S. 2001. *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace*. Cambridge: The MIT Press.

Blumenthal, M. S., and D. D. Clark. 1997. "Rethinking the Design of the Internet: The End-to-End Arguments vs. the Brave New World," *ACM Transactions on Internet Technology* 1, no. 1:70–109.

Bonnett, T. W. 2001. "Is ISP-bound Traffic Local or Interstate?" *Federal Communications Law Journal* 53, no. 2:239–287.

CompuServe Incorporated v Cyber Promotions, Inc., 962 F.Supp. 1015 (S.D. Ohio 1997).

Downes, T., and S. Greenstein. 2002. "Universal Access and Local Internet Markets in the US," *Research Policy* 31, no.7: 1035–1052.

Engel, F. 1999. "The Role of Service Level Agreements in the Internet Service Provider Industry," I*nternational Journal of Network Management* 9:299–301.

Ferrera, G. R., S. D. Lichtenstein, M. E. K. Reder, R. August, and W. T. Schiano. 2001. *Cyberlaw: Text and Cases.* Cincinnati: West/Thomson Learning.

Frydman, Benoit, and Rorive, Isabelle. 2002. "Regulating Internet Content through Intermediaries in Europe and the USA," *Zeitschrift für Rechtssoziologie* 23.

Girasa, R. J. 2002. *Cyberlaw: National and International Perspectives.* Upper Saddle River, N.J.: Prentice Hall.

Gorman, S. P., and E. J. Malecki. 2000. "The Networks of the Internet: An Analysis of Provider Networks in the USA," *Telecommunications Policy* 24:113–134.

Greenstein, S. 2000. "Building and Delivering the Virtual World: Commercializing Services for Internet Access," *Journal of Industrial Economics* 48, no. 4: 391–411.

Greenstein, S. 2001. "Technological Mediation and Commercial Development in the Early Internet Access Market," *California Management Review* 43, no. 2:75–95.

Hallman, G., and C. McClain. 1999. "Real Options Applications for Telecommunications Deregulation," in *The New Investment Theory of Real Options and Its Implications for Telecommunications Economics,* edited by J. Alleman and E. M. Noam, 139–158. Boston: Kluwer Academic Publishers.

Johnson, D. R., and D. G. Post 1996. "Law and Borders: The Rise of Law in Cyberspace," *Stanford Law Review* 48:1367–1402.

Lemley, M. A., P. S. Menell, R. P. Meges and P. Samuelson 2000. *Software and Internet Law.* Gaithersburg, N.Y.: Aspen Publishers.

Lipschultz, J. H. 2000. *Free Expression in the Age of the Internet: Social and Legal Boundaries.* Boulder: Westview Press.

Maggs, P. B., J. T. Soma, and J. A. Sprowl. 2001. *Internet and Computer Law: Cases, Comments, Questions.* St. Paul: West Group.

Menzel, D. C. (1998). www.ethics.gov: Issues and challenges facing public managers, *Public Administration Review*, 58(5), 445–52.

Noam, E. M. 2001. *Interconnecting the Network of Networks.* Cambridge: The MIT Press.

Nosworthy, J. D. 2000. "Implementing Information Security in the 21st Century," *Computers & Security* 19, no. 4:337–347.

Patel, S. K. 2002. "Immunizing Internet Service Providers from Third-Party Internet Defamation Claims: How Far Should Courts Go?" *Vanderbilt Law Review* 55, no. 2:647–91.

Phillips, J. T. 2000. "ISPs and ASPs Create New Records Issues," *Informa-tion Management Journal* 34, no. 4:61–63.

Puentes, J. P., and P. V. Rothenberg. 2001. "10 Essential Contract Terms for Broadband Service Agreements," *Journal of Property Management* 66, no. 6:43–46.

Reidenberg, J. 1996. "Governing Networks and Rule-Making in Cyberspace," *Emory Law Journal* 45:911–930.

Rosenoer, J. 1997. *Cyberlaw: The Law of the Internet.* New York: Springer.

Schruers, M. 2002. "The History and Economics of ISP Liability for Third Party Content," *Virginia Law Review* 88, no. 1:205–264.

Siau, Keng, F. F. Nahy, and L. Teng. 2002. "Acceptable Internet Use Policy: Surveying Use Policies of Three Organizations—Educational Institutions, ISPs, and Non-ISPs," *Communications of the ACM* 45, no. 1:75–80.

Townsend, A. M., R. J. Aalberts, and S. A. Gibson. 2000. "Libel and Slander on the Internet," *Communications of the ACM* 43, no. 6:16–21.

Wernick, A. S. 2001. "US Internet Service Provider Liability," *Computer Law & Security Report* 17, no. 4:247–249.

Wetzel, R. 2000) "ISP Customers Habits, Likes and Dislikes," *American Journal of Human Genetics* 7, no. 37:31–42.

Zittrain, J. 2003. "Internet Points of Control," in *The Emergent Global Information Policy Regime,* edited by S. Braman. Houndsmills, UK: Palgrave/ Macmillan.