(A) Any legislation should give at least some types of ISPs a duty to remove infringing copyrighted material from their systems.

(1) ISPs are the logical party to which to give a duty to remove infringing copyrighted material because they are so well-positioned

ISPs and access providers are uniquely well-positioned to stop the loss of intellectual property rights on the Internet. The Report of the Working Group on Intellectual Property Rights (White Paper) supports this assertion, stating:

> "On-line service providers have a business relationship with their subscribers. They -- and, perhaps, only they -- are in the position to know the identity and activities of their subscribers and to stop unlawful activities."

White Paper, at p. 117.

ISPs have the ability to dictate the online environment through the use of written control policies and guidelines. They are able to ensure that these are in place and followed.[18] They have the ability to place warnings on their networks against the posting of copyright infringing material and suspend access to groups or persons that persistent'y infringe copyrights.[19] ISPs can utilize and implement technology, including software, that is capable of automatically screening material posted on the network.[20]

Given their close relationship with their subscribers, ISPs are in the best position to receive notice of specific improper traffic and receive information with respect to specific problems in various user groups.[21] They are in a position to quickly and effectively handle

[18] NETCOM 3, at 3, 9; RTC v. FACTNET 1, 901 F. Supp. at 1521; Stratton Oakmont v. PRODIGY, 1995 WL 323710, at 3 & 4. See also "MCI Gets Tough on Spamming", Business Daily, 1/25/96.

[19] NETCOM 3 at 9; Sega at 687 (improper postings encouraged by provider). CompuServe Press Release, December 28, 1995 (access to 200 newsgroups suspended in Germany).

[20] NETCOM 3 at 3, 9-10; Stratton Oakmont at 3 & 4; Cubby v. Compuserve, 776 F. Supp 135, 140 (S.D.N.Y. 1991).

[21] NETCOM 3 at 3, 7-9; Cubby at 137, 141. See also the Bitnet letter attached.

objectionable traffic, whether it is patently improper, such as third party credit card numbers, or whether its impropriety is latent in nature.[22] ISPs are also in a position to hire intermediate editorial groups responsible for reviewing network traffic and enforcing network policies.[23]

Many ISPs are already promulgating and enforcing rules of usage by their customers and have suspended accounts in thousands of instances were abusive use has occurred. Some ISPs have begun monitoring the activities of their subscribers, recognizing the marketing significance of tracking subscriber online activity.

Therefore, ISPs have both the ability and a history of controlling certain kinds of subscriber activity. Because they are so well-positioned, ISPs are the logical party on which to place a duty to remove infringing materials on-line.

(2) ISPs, rather than the courts, should be given the duty to take offline infringing copyrighted material because ISPs provide a better first line of defense against copyright infringement than do the courts.

Considering the speed with which online infringement can utterly destroy the value of a copyright, courts are institutionally ill-equipped to prevent online copyright infringement with the required alacrity. Even the speediest court procedures, such as temporary restraining orders and preliminary injunctions, require the intervention of a middleman - the court - between the service provider and the copyright owner. Therefore, court procedures are not sufficiently immediate to prevent substantial damage from online copyright infringement. Furthermore, even where a TRO is obtained, courts are so sensitive to even poorly founded First Amendment claims that they sometimes improperly conduct the weighing analysis required for preliminary hearings.

The institutional limitations of the courts indicate that they may be a poor first line of defense against online copyright infringement. Therefore, the duty to remove infringing copyrighted material is better given to the ISPs, who, as demonstrated above, are quite well-equipped to handle this duty.

(3) There is good precedent for the government finding that ISPs should have a duty to prevent online illegal activities, such as copyright infringement

Congress would not be without precedent if it gave ISPs some level of responsibility for preventing online copyright infringement. The recently passed telecommunications bill would

[22] NETCOM 3 at 7-9; FACTNET 1, 901 F. Supp. at 1526; Playboy at 1556; Sega at 683-4; Cubby at 141. See also Tamburo v. Calvin, 1995 WL 121539 (N.D.Il. 1995).

[23] NETCOM 3 at 3; Stratton Oakmont at 3 & 5; Cubby at 137, 140.

make ISPs criminally liable for providing access to online pornography. Giving ISPs a measure of responsibility for preventing online copyright infringement is far less burdensome and intrusive than making ISPs criminally liable for online pornography.

Further precedent comes from another branch of the government. In 1990, the Commerce Department issued a letter to the administrators of the BITNET, an earlier form of the Internet. The Commerce Department concluded that ISPs were more like publishers than distributors based upon their relationship to their users, their ability to exercise editorial control, their ability to set and enforce guidelines, and their ability to respond to information provided by subscribers. Based on its findings, the Commerce Department expressed the view that ISPs may be liable for online violations of the export laws.[24]

(4) It is equitable to give ISPs a duty to remove infringing copyrighted material

Giving ISPs an explicit duty to remove infringing material from their systems would give them a greater responsibility for preventing copyright infringement than they currently have. However, I believe such an increased burden is equitable if the Internet is to remain an essentially unregulated environment. For ISPs, who run a billion dollar industry, to reap the substantial rewards of operating in an unregulated field, they should accept the responsibility to self-regulate to ensure that there is no wholesale violation of property rights online.

(5) Such a duty should not relieve ISPs of existing liability for copyright infringement

The creation of this duty should not be used to weaken the protection of copyrights overall. ISPs should still face the full range of liability for copyright infringement, whether contributory, direct or vicarious, that they face under correctly applied current law. Furthermore, the proposed duty should not change the fact that ISPs are liable for copyright infringement when they have actual knowledge of infringing material on their systems, even if that knowledge is derived from sources other than the copyright owner.

(B) The duty given to ISPs should, at the least, require that ISPs remove copyright infringing material from their systems when they have notice that such materials are on their systems

Having proposed that ISPs be given a duty to prevent online copyright infringement on their networks, the issue then becomes the exact nature of the duty.

(1) The duty should be mandatory, not voluntary.

[24] A copy of the Bitnet letter is attached.

Such self-regulation should be not be voluntary, but should be mandated through legislation. A voluntary duty would not provide sufficient protection to copyrights. While major ISPs would most likely shoulder a voluntary duty, the smaller ISPs would have a direct incentive to ignore a voluntary duty. These smaller ISPs can more effectively compete with the bigger ISPs by giving their subscribers access to content not available on the bigger systems. Therefore, as happened in the Sega case, many smaller ISPs will not act to remove copyright infringing material from their systems.

The likely compliance of only the major ISPs with a voluntary duty will not provide any protection to copyrights. If copyright infringing material is available anywhere online, it can be disseminated worldwide in a matter of minutes.

There is good precedent for making any duty on ISPs mandatory. As the White Paper itself concludes,

> "It would be unfair -- and set a dangerous precedent -- to allow one class of distributors to self-determine their liability by refusing to take responsibility. This would encourage intentional and willful ignorance."(p. 122)

(2) A reasonable duty would, at the least, require the ISPs to remove infringing copyrighted material from their systems when they have received notice that such material is on their system.

A duty to remove materials upon notice from copyright owners that such material infringes a copyright seems entirely reasonable. Besides being eminently reasonable, a duty to remove material upon notice that such material infringes a copyright has many advantages. Such a duty:

- Does not give ISPs the duty to monitor all online communications for copyright infringement, and therefore does not require ISPs to do the impossible.
- Does not require ISPs to violate the Electronic Communications Privacy Act by monitoring their postings or e-mail.
- Evenly distributes the burden of the duty by involving copyright owners in providing notice that copyright infringing material is on the system.
- Provides for direct action between the service provider and the copyright owner, and therefore will significantly speed up the process of removing infringing material.
- Has explicit support from the White Paper, which stated that

> "Service providers should have incentive to...react promptly and appropriately to notice by copyright owner that infringing material is available on their systems."

(p. 124)

(3) This duty to remove upon notice should involve sanctions for failure to comply with the duty

A duty to remove infringing materials upon notice will not be effective unless there are sanctions for noncompliance. Therefore, any legislation creating such a duty must also create sanctions for noncompliance.

(4) Arguments against imposing such a duty on ISPs are not compelling

Some ISPs have argued that copyright holders are obligated to secure their intellectual property. However, it is far more difficult for copyright owners to secure their intellectual property in the online environment than in traditional media. Copyright owners have no right, and little ability, to remove copyright infringing material from an ISP's system. Furthermore, computer hackers have been able to break into virtually all corporate and government networks by using intrusion technology like spoofers,[25] sniffers,[26] satan utilities,[27] trojan horses,[28]

[25] Professor Eugene Spafford of Purdue University, a forensic computer code expert, explains "spoofing or "IP spoofing" as follows: IP (Internet Protocol) is the standard protocol for connections on the Internet. This involves sending messages as a set of individual "packets," each with a source address and a destination address. The packets are assembled into messages that are then acted upon. A sequence number is in each packet to help identify when a packet needs to be resent, or is received multiple times.

Most programs that involve a long-term connection set up permissions and initialization when connections first occur. Thereafter, any packets arriving with the correct source and destination address, sequence number, and other per-session values are assumed to be part of the on-going connection, and are processed accordingly.

"IP spoofing" involves an attacker determining the likely values for the sequence number and other information, and then forging a series of packets that appear to be from the legitimate source of the connection. The processing host is fooled if the values are correct, and uses the packets in its connection. The result is that the person doing the "spoofing" can introduce arbitrary commands and data into the session. Under some conditions, they can actually "hijack" the connection and take over control of the session -- leaving the original source computer with no connection (because it no longer has the correct sequence numbers -- they have changed as a result of the hijacking). Spafford e-mail of December 12, 1995.

[26] Sniffers are packet-capturing programs installed on the Internet. They examine captured packets to obtain login name-password combinations for remote login sessions. This information

back doors,[29] e-mail protocol attacks,[30] and network file system attacks.[31] Copyright owners should not be penalized for the advent of new technology which permits greater unauthorized distribution of copyrighted material while restricting their ability to secure the material. Rather, where reasonable, ISPs should have a measure of responsibility for removing copyright infringing material.

Some ISPs also argue that they are entitled to common carrier status. ISPs are not similar to common carriers, however, and should not be exempted from the proposed duty. Congress has never provided ISPs with the protection of a common carrier exemption, nor should it. Giving ISPs a common carrier exemption would be the equivalent of allowing them to have their cake and eat it too. Common carriers in other fields, such as phone companies, have exemptions form certain types of liability because they also are extremely tightly regulated and have a host of legal duties. The rates they may charge are regulated, they generally are not allowed to deny access to anyone, and they have to comply with voluminous regulations regarding the conduct of their business.

is then used to log into the hosts across the network for which the packets were destined. "Internet Sniffer Attacks," Eugene Schultz and Thomas A. Longstaff, 18th NISS Conf. Proceedings, Oct. 10-13, 1995, p. 535. Sniffer attacks involve scanning for reusable passwords, gaining root access to a network system, and replacing detection tools with Trojan horse utilities. CERT, November, 1995.

[27] Satan is a widely available Unix computer security tool that can scan a network environment looking for 13 known TCP/IP vulnerabilities. Difficulty develops when system administrators rely on the results of the Satan examination and fail to respond to new vulnerabilities in TCP/IP being trafficked in the computer underground.

[28] A Trojan horse is a program that disguises its harmful intent by purporting to accomplish some harmless and possibly useful function. For example, a trojan horse program could be advertised as a calculator, but it may actually perform some other function when executed such as modifying files or security mechanisms. A computer virus could be one form a trojan horse. John Wack, NIST, September 22, 1989.

[29] Back doors are entry points to a program or system that are hidden or disguised. They are often created by the software's author for maintenance or other convenience reasons. For example, an operating system's password mechanism may contain a back door such that a certain sequence of control characters may permit access to the system manager account. Once a back door becomes known, it can be used by unauthorized users or malicious software to gain entry and cause damage. John Wack, NIST, September 22, 1989.

[30] CERT, November, 1995 and DOD Assist Project.

[31] CERT, November, 1995 and DOD Assist Project.

If ISPs want the benefits of a common carrier exemption, they must accept the tight regulation that accompanies it. However, tight regulation coupled with exemption from liability is not what the ISPs propose when they clamor for a common carrier exemption. The last thing the ISPs want is to become tightly regulated entities, with the government dictating their fees and terms of agreement. Instead, they ask for the benefits of a common carrier exemption, but want to avoid the responsibilities and burdens that generally come with common carrier status.

If they are to remain almost totally unregulated, I believe it is only right that ISPs be given a legal duty to self-regulate, at least to the extent involved by the proposed duty.

Some ISPs have argued that the First Amendment rights of subscribers would be violated by full enforcement of copyright law online. The enforcement of copyright law online through the imposition of an affirmative duty to remove copyright infringing material is no more a violation of free speech than are attempts to enforce copyright law in any other media. By definition, copyright law always gives one individual an exclusive right to express ideas in a certain way, and therefore restricts the ability of all others to use the same expression.

Furthermore, First Amendment concerns are addressed in the copyright law by the assurance of a fair use defense against claims of infringement. Case law has recognized that to the extent that First Amendment rights outweigh any exclusive rights granted by the Copyright Act, the protections afforded by the fair use defense are adequate.

VII. Conclusion

In conclusion, I wish to state my firm belief that the creation of such a reasonable duty will more effectively prevent online copyright infringement than current law in at least those narrrow circumstances in which the copyright owner is aware of the infringing material and gives notice to the ISP. Surely, those whose intellectual talent has made this nation the world's creative leader deserve no less.

I do not suggest that the creation of a duty similar to that proposed in this testimony will provide a panacea to the problem of online copyright infringement. Rather, I see the proposed duty as one of the most obvious ways to improve copyright protection online. Other mechanisms, whether legislative, technological, or enforcement-oriented, are needed to more completely protect copyrights against on-line infringement.

Mr. MOORHEAD. Ms. Simmons-Gills.

STATMENT OF CATHERINE SIMMONS-GILL, PRESIDENT, INTERNATIONAL TRADEMARK ASSOCIATION, AND GENERAL COUNSEL, GENERAL MEDIA INTERNATIONAL, INC.

Ms. SIMMONS-GILL. Thank you, Chairman Moorhead, and members of the panel. I am here today to speak on a topic that no one else has spoken of, I think, in the past couple of days and that is the issue of domain names and trademarks on the Internet. But before I do that, I would like to thank the chairman and you, Mrs. Schroeder, for your help in the passing of the—and the recent enactment of the trademark dilution statute, which became law on January 16. We are very grateful for your assistance in that regard.

My principal message to the panel today is that the current policies associated with the registering of domain names, sort of like a post office address on the Internet, are in need of some serious attention by all the constituent communities that deal with them. I think we have had some very helpful description of the mechanics of the Internet. I would like to speak just a little bit about the history of the Internet, which began as a means of communication that was safe from various intrusions between the Department of Defense, its contractors, and then later think tank scientists and universities.

Of course, over the past 5 years, it has become much more commercialized than that, and involves many, many hundreds of thousands of providers. Each of these providers has an address, which is a numeric address, and in addition, they have a gnomonic device or a domain name which is the way you get to that person, and addresses which are numbers are matched up with names.

Prior to 1993, the total number of names issued in a year was approximately 10,000. Now, even though the process is painstakingly slow, they are issuing 13,000 a month. So many, many names are being issued.

The problem is that names are issued randomly more or less on a first come, first served basis and you get the name that you ask for unless someone else has an identical name on the Internet. This has led to a variety of instances of confusion when names such as Avon or McDonald's are issued to parties that are unrelated to the entities best known by the most members—most members of the public as Avon or McDonald's.

The *McDonald's* case is sort of interesting. A Newsday reporter called McDonald's and found out, in fact, that they had not applied for a domain name involving McDonald's, and he applied for and obtained the name ronald@mcdonalds.com. There was then a reasonably friendly discussion between this reporter, who was doing it for reporting purposes, and in return for a substantial donation to a New York City school McDonald's got its name back.

This was done to prove a point, but many of these names are obtained to prove other points. Specifically, a case was recently filed by Avon against an individual in New York who indicated that she had intentionally acquired the name Avon in order to get Avon to pay her a sum of money to obtain its own name on the Internet.

And some of them are just, quite frankly—there are people whose surname is McDonald's or Sears or whatever, and they applied for and obtained their own name.

So there—we have the Internet name provision system, which is flat first come, first served. And then you have the whole world of trademark law, which is global, horizontal in some ways but vertical in others. There is Acme—there may be Acme for paints and Acme for food. There is Cadillac electronics, Cadillac for automotive—for cars, and Cadillac for other products as well.

We certainly understand why this situation came to be and we believe it needs to be addressed. Domain names are issued by NSI. We have handed out a chart. This chart was actually put out by RIPE–NCC. RIPE–NCC is one of the creators of Internet names in Europe, actually. We have marked in blue who we know—what we know what they are. And we do know some of the purples. We have no idea who WWW Society is, but we guess that it is the World Wide Web Society.

All of these groups are the groups that together provide the Internet for all of our use. And they are doing a good job, and they have done a good job, but it is on an ad hoc voluntary basis.

Limiting myself to the issue of domain names and trademark infringement, when this problem was brought to the attention of NSI, who issues names, they undertook to provide a policy which was amended once last year. It was provided last year and amended once. And basically, they have—the policy says that if someone gets a domain name and the owner of the trademark is able to provide NSI with a trademark registration certificate, showing first use for exactly the same name prior to that time, then they will ask the person issued the name to stop using it. And if he or she won't stop using it voluntarily, they will suspend, send the thing to arbitration in California and at the end of the arbitration issue the name to whoever it is that has prevailed in the arbitration.

In the 9 months we do not know of a single situation that has been resolved in this fashion. Some have been resolved in the sort of Newsday way, where they came to—others have been negotiated in other ways and there are a couple of cases pending. Meanwhile, of course, many more names are being issued.

What is our suggestion under these circumstances? Our suggestion under these circumstances is, first of all, that the committee understand, of course, that—the subcommittee understand that the Internet is global. It is absolutely guarded and maintained by a group of engineers who have done an extraordinarily good job and who are very concerned about being overregulated and over legislated, but to whom we are indebted and who we will need to count on to fix problems.

So we would like to recommend specifically that this committee or Congress urge that a group be created composed of engineers that are actively involved and well-respected in the Internet and there are several—there are many of these; of trademark owners and businesses that are involved in this commercial aspect; of some people or one or two members that just use the net so they would be consumers and would understand the issues of the public being confused by this proliferation of names, and finally of groups that are specifically interested in trademarks, like the International

Trademark Association, or WIPO, who would within 6 to 10 months come up with some solution for the issuance of domain names that addresses, insofar as possible, on a reasonable basis and a global basis and an engineeringly sound basis the problem of domain names.

It is not only a U.S. problem, although most of the traffic for the Internet does go through the United States and most people, although not all, are obtaining names through U.S.—through the U.S. entity NSI. We do think that this can be addressed at the urging of this committee and of Congress.

Thank you.

[The prepared statement of Ms. Simmons-Gill follows:]