Testimony of

Jon Weinberg

Professor of Law, Wayne State University

Detroit, MI 48202

(313) 577-3942

before the

Commission on Online Child Protection

June 8, 2000

Executive Summary

It would be untenable for the United States government simply to order the creation of a new top-level domain for material harmful to minors. Rather, if the U.S. government wishes to see such a domain created, it will have to work within the ICANN policy process. The benefits of having such a domain, though, are clouded at best. If use of the domain is not made mandatory, its mere existence will do little to reduce access by minors to sexually explicit material on the World Wide Web. But any statute purporting to make use of the domain mandatory would raise serious constitutional problems.

Prepared Testimony

Mr. Chairman and members of the Commission, I am very glad to be here today. I=m going to testify today wearing two hats. First, I=m the chair of an ICANN working group on the addition of new Internet top-level domains. Second, I=m a constitutional law professor at Wayne State University and the author of an article on Internet filtering software. I=m not speaking, though, on behalf of either ICANN, the working group or Wayne State University; rather, I=m speaking only for myself.

Background

I want to start by providing some background on the management of Internet names and addresses. Internet resources are typically identified by *domain names* such as www.copacommission.org. The domain name space is divided into top-level domains, or TLDs; each TLD is divided into second-level domains, or SLDs; and so on. Under a plan developed in 1984, there are seven Ageneric,≅ three-letter top-level domains: .com, .net, .org .edu, .gov (reserved for U.S. government sites) .mil (reserved for U.S. military sites), and .int (reserved for intergovernmental organizations). In addition, there are a whole lot of two-letter Acountry code≅ top-level domains, such as .jp, .us and .fr.

When a user, looking for a particular Internet resource, types in a domain name, his computer looks to a set of local *domain name servers* that are specified within its software to find the Internet address corresponding to that domain name. Those local servers, if they don=t know the answer, will kick the problem up to a higher level. At the top of the pyramid are a set of *root servers*. Whether a top-level domain is visible in the name space is determined by whether the root servers contain an entry corresponding to that domain. If a user types in a domain name incorporating a top-level domain that the root servers he consults don=t recognize, then his computer will be unable to find any resource corresponding to that domain name.

Since 1992, the job of administering the AA≅ root server, from which all of the other root servers take their lead, has been undertaken by Network Solutions, Inc., a private company, under cooperative agreements with the National Science Foundation and the Commerce Department. Since well before NSI entered the scene, overall policy oversight of the domain name system was in the hands of Dr. Jon Postel at the University of Southern California, under a contract with the Defense Department. NSI followed the directions of Dr. Postel in maintaining, and making changes to, the root servers.

This system, however, wasn=t stable. For one thing, as the Internet became increasingly international, it was incongruous for its management to be funded by U.S. government agencies charged with overseeing scientific research projects. Other countries saw the Internet as a global resource, not subject to the narrow whims of the U.S. government, and demanded a voice in its

governance. For another thing, the existing domain-name management functions had no robust management structure and no formal accountability to the Internet community.

Finally, the domain-name system was facing policy choices that were beyond the ability of the old system to resolve. Some people wanted to add many new top-level domains to the root zone; others opposed this. Some wanted the domain-name registration process to incorporate strong protection for trademark owners against the registration of names similar to their trademarks; others urged that these disputes should be left to the courts. Many people urged that other firms should be able to compete with Network Solutions in the business of registering domain names, but there was considerable argument over how this should be done. Different people suggested the creation of different new entities to help resolve these issues. These issues were thrashed out, for a period of several years, in what was sometimes called the ADNS wars.≅

The United States government took a step towards resolving these issues by midwifing the birth of a new, private, nonprofit corporation, with an internationally representative board, called ICANN X the Internet Corporation for Assigned Names and Numbers. The government announced that it would work with ICANN to transfer policy authority over the domain-name system, and specifically charged ICANN with developing policy for the addition of new top-level domains. Initially, the U.S. government proposed that even before ICANN was formed, the government should require the addition of five new top-level domains. In its final policy

statement, called the White Paper, though, the government reversed that position. It concluded that it was better for ICANN to make these decisions itself, based on global input. The White Paper noted that Athe challenge of deciding policy for the addition of new domains will be formidable.≅ It expressed support for new domains, but cautioned that Ain the short run, a prudent concern for the stability of the system suggests that expansion of [top-level domains] proceed at a deliberate and controlled pace to allow for evolution of the impact of the new [top-level domains] and well-reasoned evolution of the domain space.≅

ICANN has since engaged in extensive deliberation relating to the possible creation of new top-level domains. In April, the body responsible, within ICANN, for originating policy recommendations on domain-name issues recommended to the ICANN Board that a limited number of new top-level domains be created, in the short term, in a measured and responsible manner. It referred to the possibility of introducing Afully open top-level domains, restricted and chartered top-level domains with limited scope, non-commercial domains and personal domains.≅ It cautioned, however, that there must be Aa responsible process for introducing new gTLDs, which includes ensuring that there is close coordination with organizations dealing with Internet protocols and standards.≅

It=s not at all clear that this whole process will go smoothly. ICANN is still feeling its way, and not all players in the Internet arena fully accept its authority. The U.S. government, indeed, hasn=t yet relinquished its own policy authority over the root.

Feasibility

In one sense, it would be Afeasible≅ for Congress to order, tomorrow, the addition of a top-level domain specifically intended for material harmful to minors. Both Network Solutions and ICANN are subject to U.S. jurisdiction. Congress could order Network Solutions to add the new domain to the root servers, and to host the new domain=s registry; or it could order ICANN to find a registry to host the new domain, and to request NSI to make the appropriate root server modification. Congress has the raw power to do that.

From the standpoint of the transition of domain-name policymaking authority to ICANN, though, such a move would be disastrous. ICANN is still finding its credibility as a body, independent of national governments, to govern Internet identifiers on behalf of the Internet community. For Congress to short-circuit ICANN=s processes, ordering a particular top-level domain deployed without regard to ICANN=s own choices, would strip the ICANN process of its integrity and would make it much harder for anyone to take ICANN seriously as an independent entity for Internet technical management.

Further, this would not be the end of government involvement in ICANN decision-making. Other governments would feel entitled to have their own preferences reflected in the domain name space. Other governments would come to ICANN and insist that there be top-level domains created to reflect their own policy preferences. Given the range of speech favored and

disfavored by various world governments X including speech promoting Naziism or hate, speech tarnishing the Muslim religion, and so on X it is easy to imagine multiple calls by a wide range of governments for special top-level domains for speech they want to see ghettoized. Indeed, some governments would likely go farther and ask that ICANN use its own bureaucratic apparatus to enforce rules governing who could and could not register in a given domain.

This would damage the U.S. government=s effort to transfer domain-name management to a representative, bottom-up, private organization that could expand the name space while imposing minimalist rules. It could contribute to ICANN=s failure X and if ICANN fails, one likely result is a splintering of control, with the emergence of new sets of root servers not subject to U.S. authority at all. Alternatively, it could place irresistible pressures on ICANN to become a vehicle for the policy preferences of other world governments, each of them hostile to a different category of speech.

The bottom line is that if the U.S. government were to seek the creation of such a top-level domain as part of the global name space, it would be necessary to work within the ICANN process; it would be destructive to seek to impose that directive from without. Working within the ICANN process, I=ll warn you, is difficult, slow and contentious. Further, it=s not at all clear how ICANN would appropriately structure such a domain as part of a global name space. I understand that Roger Cochetti will be discussing some of the issues that would arise in that context, so I=ll not linger long on them here. Since I am a scholar of filtering and constitutional

law, though, I do want to discuss some of the consequences of having this sort of top-level domain at all.

Consequences

To the extent that particular web sites are located only in a particular top-level domain, the enterprise of filtering those sites would be trivial. We would see extensive new filtering, I believe, on routers and servers. That is, if there were a .XXX domain, I expect that a substantial number of Internet service providers would choose to make resources in that domain completely unavailable to their users. Indeed, a significant number of countries would do the same. This would be sufficiently effective, in limiting the commercial reach of sites located in such a domain, that I would expect relatively few U.S.-based sites would voluntarily move there, discontinuing their presence in .com. (On the other hand, some might well move there while maintaining an identical presence in .com.) No sites based outside the U.S. would discontinue their existing sites. The upshot is that the establishment of such a domain, without more, would do little to reduce access by minors to sexually explicit material on the World Wide Web. Any value it had in facilitating filtering would likely be outweighed by its disadvantages in providing to some minors a sure-fire way of finding sexually explicit materials.

The regulatory alternative would be to make use of the domain mandatory -- that is, to make it illegal for U.S.-based speakers to distribute certain categories of speech via the World

Wide Web, except at a web site located in the particular top-level domain. This would raise substantial first amendment issues, though. As I mentioned a moment ago, a site located in such a domain would have vastly smaller reach X a substantial number of ISPs would not make it available at all. While individual users would not have to subscribe to those ISPs, a user might well find that if he wanted access to a particular site, he would have to change ISPs in order to do so. Further, any site located in that domain would immediately be branded, in the public eye, as pornography. As a result, requiring a particular speaker to locate in the Aharmful to minors≅ top-level domain would substantially interfere with his ability to get his message out.

This would, in turn, raise all of the first amendment issues that arose in the *Reno v. ACLU* and COPA litigations. How should the class of speakers to be exiled to this domain be defined? Recall the Supreme Court=s question in *Reno v. ACLU*: ACould a speaker confidently assume that a serious discussion about birth control practices, homosexuality, the First Amendment issues raised by the Appendix to our Pacifica opinion, or the consequences of prison rape would not≅ be covered by the statute? Speakers would have reason to fear, the Court continued, that a prosecutor would read the statute to extend to discussions about safe sexual practices or artistic images including nude subjects. It seems to me plain that it would be unconstitutional to require speakers like those to exile themselves, on pain of criminal prosecution, to a top-level domain from which they could not realistically be heard. That means, though, that such a statute would face the same sort of constitutional obstacles as have prior statutes in this area.

Conclusion

In sum: It would be untenable for the United States government simply to order the creation of a new top-level domain for material harmful to minors. Rather, if it wishes to see such a domain created, it will have to work within the ICANN policy process. The benefits of having such a domain, though, are clouded at best. If use of the domain is not made mandatory, its mere existence will do little to reduce access by minors to sexually explicit material on the World Wide Web. But any statute purporting to make use of the domain mandatory would raise serious constitutional problems.

I hope this testimony has been helpful. I stand ready to answer any questions you have.