UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

CENTER FOR DEMOCRACY & TECHNOLOGY, *et al.,*

Plaintiffs,

v. No. 03-5051

MICHAEL FISHER, Attorney General of the Commonwealth of Pennsylvania,

Defendant.

MEMORANDUM IN SUPPORT OF PLAINTIFFS' MOTION FOR DECLARATORY RELIEF AND FOR PRELIMINARY AND PERMANENT INJUNCTIVE RELIEF

John B. Morris, Jr., Esq.
Lara M. Flint, Esq.
Center for Democracy & Technology
1634 I Street, NW, Suite 1100
Washington, D.C. 20006
(202) 637-9800

Stefan Presser, Esq.
Bar No. 43067
Legal Director
American Civil Liberties Union
of Pennsylvania
125 South Ninth Street
Suite 701
Philadelphia, PA 19107
(215) 592-1513 ext. 116

Seth Kreimer, Esq.
Bar No. 26102
3400 Chestnut Street
Philadelphia, PA 19104
(215) 898-7447

Dated: December 12, 2003

TABLE OF CONTENTS

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

CENTER FOR DEMOCRACY & TECHNOLOGY, *et al.,*

Plaintiffs,

v. No. 03-5051

MICHAEL FISHER, Attorney General of the Commonwealth of Pennsylvania,

Defendant.

MEMORANDUM IN SUPPORT OF PLAINTIFFS' MOTION FOR DECLARATORY RELIEF AND FOR PRELIMINARY AND PERMANENT INJUNCTIVE RELIEF

In this case, the Pennsylvania Legislature and the Defendant Pennsylvania Attorney General have taken a new and untested approach to respond to what is unquestionably an important problem in our society – child pornography. The Plaintiffs here completely agree that fighting child pornography – on the Internet and off – should be a significant governmental goal, and that those responsible for the creation or posting on the Internet of child pornography should be prosecuted to the full extent of the law.

The Legislature's and Defendant's approach, however, fails to take into account the technical realities of the Internet, and that failure has led to the direct governmental censorship of a truly massive, unprecedented amount of lawful, constitutionally protected speech. Discovery to date in this case has documented that well over *one million* web sites have been blocked by the Defendant's actions here, and that over six hundred thousand of those web sites remain blocked today (with many more historic and current blocked sites as yet unidentified). To Plaintiffs' knowledge, never before in the history of the United States has protected expression been

blocked by governmental action on such a massive scale and for such a duration as presented here.

The Legislature's and Defendant's approach runs directly into, and plainly violates, constitutional principles established and reaffirmed long before the Internet emerged as a vital communications medium in our society. The courts – first the Eastern District of Pennsylvania and then the United States Supreme Court – have squarely established that speech on the Internet warrants the highest level of constitutional protection afforded by the First Amendment. This case presents for the first time the vital question of how that constitutional protection will be applied to the specific technical features, such Uniform Resource Locators and Internet Protocol Addresses, that underlie virtually all communications over the Internet.

As set out below, Plaintiffs believe that the application of long standing "off-line" legal principles under the First and Fourteenth Amendments and the Commerce Clause of the U.S. Constitution to the new "online" communications techniques will require the Court to declare the Pennsylvania statute challenged here to be unconstitutional, and to permanently enjoin both the enforcement of that statute and the perpetuation of the secret, non-statutory system of blocking orders devised and implemented by the Defendant.

NOTE CONCERNING REDACTED WEB SITE NAMES

On September 12, 2003, the Court entered a Protective Order restricting the dissemination of the Internet addresses ("Uniform Resource Locators" or "URLs") of alleged child pornography targeted by the Defendant in his Informal Notices. Pursuant to that Order, Plaintiffs have redacted from this brief critical elements of any URLs covered by the Protective Order, and have substituted for them the term "RedactedURL" followed by a number. Thus, a hypothetical URL "www.example.com" might, if covered by the Protective Order, appear in this

brief as "www.RedactedURL6.com." Plaintiffs will also file under seal with the Court a document that translates the redacted URL back to the unredacted form. Using this method, Plaintiffs have been able to include the maximum amount of information on the public record. The exception is where the blocking orders have required the blocking of access to well-known online communities such as www.terra.es. In such cases Plaintiffs have not redacted the "www.terra.es" but have redacted the most essential element of the subpages of the URL.

The Court's order only covered the confidential URLs, and did not address the numeric "Internet Protocol" (or "IP") addresses that have been blocked by the ISPs. In some (but far from all) situations, an IP address can be used to access a web site hosted at the IP address. Plaintiffs have not redacted any IP addresses, however, for the simple reason that in all relevant cases the confidential URL no longer resolves to the blocked IP address, and thus there is no risk that the IP address could be used to lead back to the confidential URL.

FACTUAL BACKGROUND

The goal of both the challenged statute and the Defendant's implementation of the statute through "Informal Notices" – fighting child pornography – is clearly a laudable and important one. It is also clear that neither the Legislature nor the Defendant set out to censor or block access to constitutionally protected web sites, much less over a million such web sites. But however well-intended the statute and Informal Notices may be, the method used by the statute (and perpetuated in the Informal Notices) has led to censorship on a truly massive scale. At the same time, as detailed below, neither the statute nor the Informal Notices actually further any appropriate governmental interest.

Because "the loss of First Amendment freedoms, for even minimal periods of time,

unquestionably constitutes irreparable injury,"[1] Plaintiffs have sought to expedite the proceedings in this case, and the Court has ordered a period of expedited discovery and has scheduled an early trial date. Many of the facts discussed below have already been placed before the Court in support of prior motions. Many other relevant facts addressed below, however, have not been previously documented, and will be established at trial. Where possible, Plaintiffs provide below citation to the previously submitted evidence.

As this Court is well aware, this case involves some very specific technical details about the Internet. The expert reports prepared by the three expert witnesses in this case (Plaintiffs' experts Mitchell Marcus and Michael Clark, and Defendant's expert Benjamin Stern) all provide helpful technical background about the Internet. In particular, the report of Professor Marcus, the former chair of the Department of Computer and Information Science of the University of Pennsylvania, provides an expert overview – at Paragraphs 6-39 of his report – of how the Internet operates, of how the World Wide Web operates, and of the definition of key terms like URL, domain name, and IP address.[2]

Plaintiffs have sought below to provide an overview of the relevant facts, but discovery in this case continues for a brief period following the submission of this brief (one critical deposition took place the date of this brief, and one is scheduled for early next week). Thus, this overview cannot be a comprehensive detailing of the all relevant facts, and Plaintiffs expect that the parties' stipulations and Plaintiffs' proposed findings of fact will include facts and citations not set out below.

---

[1] *Elrod v. Burns*, 427 U.S. 347, 373 (1976).

[2] The report of Professor Marcus and the two reports of Michael Clark were submitted as Exhibits 1, 2, and 3 in support of Plaintiffs' Motion For A Supplemental Temporary Restraining Order And/Or For Supplemental Preliminary Injunctive Relief, filed Dec. 2, 2003 (hereafter "Supplemental TRO Exhs.").

A. The Statute

The statute challenged in this action imposes potential liability on Internet Service Providers ("ISPs") for child pornography available on the Internet, even if the ISPs are not hosting the offending content and have no relationship whatsoever with the publishers of the content. *See* 18 Pa. Stat. Ann. §§ 7621-7630 (the "Statute," the full text of which is attached to the Complaint).[3] The law permits the entry of a court order requiring an ISP to block or disable Pennsylvanians' ability to access specified content alleged to be child pornography. *Id.* § 7622. The entire court proceeding can go forward on an *ex parte* basis, with no prior notice to the ISP or the web site owner required, and no post-hearing notice to the web site owner. *Id.* §§ 7627-7628. Moreover, a court order under the Statute need only be based on a "probable cause" finding that there exists evidence that certain Internet content violates the law. *Id.* § 7627.

The Statute has to date only been used one time. In September 2002, the Attorney General obtained an *ex parte* probable cause order against the Internet Service Provider WorldCom, after WorldCom indicated in July 2002 that it would not comply with the statutorily-unauthorized and secret "Informal Notice" orders described below. The court order was titled "Order Requiring an Internet Service Provider to Remove or Disable Access to Child Pornography," and was entered on September 17, 2002, by the Court of Common Pleas of Montgomery County, Pennsylvania, in *In the Matter of the Application of D. Michael Fisher, Attorney General of the Commonwealth of Pennsylvania for an Order Requiring an Internet Service Provider to Remove or Disable Access to Child Pornography*, No. Misc 689 Jul 02, Ct. Cm. Pleas, Montgomery County, Pa.

Under the statutory scheme, the content to be blocked is identified solely by the

[3] The law was originally enacted at 18 Pa. Stat. Ann. § 7330, but was re-codified to 18 Pa. Stat. Ann. §§ 7621-7630.

"Uniform Resource Locator" (or URL, such as http://www.cdt.org) of the World Wide Web site on which the alleged child pornography is located at the time of the application for the blocking order. Orders under the Statute do not provide any additional designation of what content should be blocked. The Order entered in the WorldCom case does not, for example, require the blocking of access to "a movie entitled 'Hot Video' located at Uniform Resource Locator www.example.com" or "a photograph depicting [a specific scene] located at Uniform Resource Locator www.example.com." Instead, for example, the WorldCom Order requires the blocking of all present and future content that might be located at a particular location on the Internet, http://www.RedactedURL2.biz,[4] regardless of whether the content presented to the state court remains at that URL.[5]

The Statute also lacks any provision for any subsequent or continuing review of any URL blocked pursuant to the Statute. Thus, the Order entered in the WorldCom case effects a permanent prohibition on access to any content located at the specified URLs, regardless of whether the content at the URLs changes after the application for the court order is filed.

B. The Informal Notice Scheme

Although the procedures set out in the Pennsylvania statute are quite limited (and as argued below, constitutionally insufficient), the Attorney General bypassed even those procedures (until this Court's September 9, 2003 Order enjoining additional Informal Notices).

---

[4] The URLs blocked in the WorldCom order were in fact identified in the public court record, so they likely would not need to be redacted from the brief. To be internally consistent, however, Plaintiffs have redacted those URLs as well.

[5] Some URLs blocked by the WorldCom order did contain a specific sub-page designation, such as for example, http://www.RedactedURL3.com/two.html, where the "two.html" referred to an HTML file that controls the formatting of words and images of a subpage on the web page. Because of the dynamic and ever-changing nature of the Internet, however, a mere reference to a particular HTML page is as ephemeral as a reference to a URL without a specific HTML page listed. Just as what is located at the

Instead of obtaining court orders under the Statute, he used a system of "Informal Notices" that he alone issues to ISPs, without any judicial or public oversight. In the more than 500 Informal Notices he has issued since the spring of 2002, the Attorney General instructed an ISP to block access to one or more specific sites on the Internet's World Wide Web, designated by the site's URL. The Attorney General ordered the ISP to "remove or disable access to those items identified as child pornography to your subscribers who subscribe to your service from an address located within the Commonwealth of Pennsylvania within five business days of receipt of this notice."[6]

The Attorney General operated his Informal Notice system in complete secrecy. He issued the Informal Notice orders without any judicial review, either before or after they were sent out. No ISP or web site received any prior notice before the Attorney General issued the orders, and no ISP or web site was afforded an opportunity to participate in any adversarial proceeding prior to or after the issuance of an order. The Attorney General provided no notice to the affected web sites even after the issuance of a Informal Notice. Not only was the general public not informed about what content was blocked, it was not notified that content was blocked at all.

As with orders under the Statute, the Informal Notices did not in general identify any specific items of child pornography by name or description, but instead simply referenced a Uniform Resource Locator, or URL.[7] And, as with statutory orders, the Informal Notices also

---

http://www.RedactedURL3.com can change daily, hourly, or even more frequently, the content located at URL http://www.RedactedURL3.com/two.html can change at any time.

[6] For redacted copies of some of the Informal Notices, see Exhibit 1 filed on September 9, 2003, in support of Plaintiffs' first TRO motion (hereafter "TRO Exh.").

[7] As with the statutory order discussed above, some of the Informal Notices specify a subpage located at the URL, but those subpage references can change as easily as the main site itself. In a very limited number of cases, the Informal Notice specified an individual graphic image file instead of a HTML web page. For

impose a perpetual prohibition on access to any current or future content that is located at a specific URL, without regard to whether the content changes over time.

C. The Impact on the Internet and Protected Expression

In the face of Plaintiffs' Motion for a Temporary Restraining Order, the Defendant agreed to temporarily halt his Informal Notice system on September 9, 2003. Yet the one statutory order and all of the more than 500 Informal Notices imposed on ISPs remain in effect, and the unconstitutional impact of those Notices on protected expression is far-reaching.

From early on and continuing through today, the ISPs' compliance with the Informal Orders directly led to the blocking of innocent web sites. Of the four deposed ISPs that received significant numbers of Informal Notices, *all four* testified that their compliance with the Notices led to the blocking of innocent content. For example, Chris Bubb of America Online testified that that one single Informal Notice led to the blocking of 400,000 unrelated web sites. *See* Rule 30(b)(6) Deposition of America Online, Inc. (Chris Bubb), Oct. 27, 2003, excerpts in Supplemental TRO Exh. 8 (hereafter "AOL Dep."), at 54-62. In another incident, AOL blocked tens of thousands of web sites hosted by a company named About.com. *See id*. at 147-48.

Similarly, Scott Lebredo of Verizon testified to an incident in which (according to an Attorney General staff member) "upward of 500,000" web sites were blocked as a result of an Informal Notice requiring that Verizon deny access to a web site on the www.terra.es domain. *See* Rule 30(b)(6) Deposition of Verizon, Inc. (Scott Lebredo), Oct. 3, 2003 (pages 1, 14-21), excerpts in Supplemental TRO Exh. 12 (hereafter "Verizon/Lebredo Dep."), at 57-62, 106-08;

---

example, Informal Notice 7886 dated on August 26, 2003, instructed Verizon to block access to http://www.terra.es/personal9/RedactedSubpage1/pic12.jpg. The "pic12.jpg" refers to a specific image file that apparently existed in August 2003 on a particular subpage of the online community www.terra.es. A particular image file, however, can be replaced with a file of the same name but different content, and thus there is no way for anyone later reviewing the Informal Notice to determine whether the content blocked has changed.

Electronic mail message dated 9/13/02 from John Burfete to Dennis T. Guzy, Dennis. J. Guzy, and Peter Sand, all of the Attorney General's office. *See also* Rule 30(b)(6) Deposition of Comcast, Inc. (Gary Lipscomb), Oct. 23, 2003, excerpts in Supplemental TRO Exh. 9 (hereafter "Comcast Dep."), at 37-38, 49-50, 65-67 (describing the blocking of content other than what was targeted in the Informal Notices); Excerpts of Rule 30(b)(6) Deposition of Epix.com (Gary Basham), Oct, 22, 2003, excerpts in Supplemental TRO Exh. 10 (hereafter "Epix/Basham Dep."), at 74-79 (describing blocking of unrelated web sites); Excerpts of Rule 30(b)(6) Deposition of Epix.com (Susan Butchko-Krisa), Oct, 22, 2003, excerpts in Supplemental TRO Exh. 11 (hereafter "Epix/Butchko-Krisa Dep."), at 9-22 (same).

In all of the instances discussed in the depositions, the affected web sites or web hosting companies noticed the blockage and complained to the blocking ISP, and those ISPs removed the blocks that interfered with lawful content. Discovery in this litigation, however, has confirmed that a immense amount of lawful content continues to be blocked *today*. In support of their December 2, 2003, motion for additional injunctive relief, Plaintiffs submitted to the Court their multivolume Responses to Defendant's Second Set of Interrogatories. In those sworn discovery responses, Plaintiffs list *more than 600,000* individual web sites that have been and continue to be blocked as a result of the Informal Notices. *See* Supplemental TRO Exh. 15, Response to Interrogatory 1.

There is, as one might expect, a great diversity of content within the mass of blocked web sites. Among the blocked sites are, for example:

- http://isladeesculturas.tuportal.com/page2.html (a guide to certain Spanish "Islands of Sculpture")

- http://cazurro.tuportal.com/webs/index.html (a directory of governmental, cultural, political, social, and tourist resources relating to the city of Leon, Spain)

- http://digilander.libero.it/cmi/press/quotes/pressquoteseng.html (reviews of the works of opera diva Alice Baker)

- http://digilander.libero.it/joseluischilavert/eng/ (a website dedicated to the Paraguayan soccer goalkeeper José Luis Chilavert, who apparently is "the best goalkeeper of the century")

- http://www.br1sarlo.com/ (a web designer in Uruguay)

- http://club.imagenysonido.com/asetai/venticinco.htm (a Spanish translation of some writings of Chinese philosopher Tao Te Ching)

- http://www.movieposterforsale.us/afiliado8.htm (a web page describing a vendor of "family edited" DVDs that have nudity and other content removed)

That these and other web sites are blocked is established by the Third Testimony of Michael B. Clark (Supplemental TRO Exh. 4), and the Verification of Alexander Roszko (Supplemental TRO Exh. 5). Both exhibits attached screen shots showing that the web sites are unavailable over either AOL or Comcast, but are uncensored and available over an alternate ISP.

The Verification of Laura Blain demonstrates the grass roots impact of the Defendant's Informal Notices. *See* Supplemental TRO Exh. 6. As Blain describes, she is the President of a non-profit community recreation center located in Bradford County, Pennsylvania. In July 2003, the recreation center's web site was suddenly inaccessible over the Epix ISP. After a week of investigation, Blain determined that Epix was, for some reason, blocking access to the IP address used by the recreation center web site (and many other web sites as well). Upon complaining to Epix, Blain was told that the site was blocked as a consequence of a child pornography investigation conducted by the Defendant. In deposition of Epix, Susan Butchko-Krisa confirmed that the blocking of Blain's web site was blocked as response to an Informal Notice challenged in this case. *See* Epix/Butchko-Krisa Dep. at 9-22.

While a significant percentage of the more than 600,000 web sites that Plaintiffs can document are blocked today appear to be based outside of the United States, the evidence at trial

will show that over the course of the Informal Notice process, a huge quantity (almost certainly in excess of 100,000 sites, and likely many more) of U.S. web sites have also been blocked as a result of the Informal Notices. The difference between the U.S. and foreign sites is that it appears that the blockage of U.S. located sites was noticed (and thus unblocked) more quickly than the blockage of the foreign sites.

D. The Technical Causes of the Blockages

To understand the technical reasons that the extensive blockage of web sites occurs, it is important to understand how the ISPs have complied with the Informal Notices. Discovery has shown that ISPs have used two different technical methods to comply with the Notices. Of the five ISPs deposed to date in this litigation, all five used in the first instance the technique of "null routing" an IP address[8] (and the largest retail ISP in the world, AOL, testified that null routing was the *only* method of compliance possible on its network[9]). In addition, two of the five also used the technique of "poisoning" or "spoiling" the "DNS cache."[10]

Plaintiffs' expert Professor Mitch Marcus has reviewed the relevant portions of the depositions of the ISPs, and at Paragraphs 54-67 of his Expert Report and Testimony, he explains and illustrates the two techniques used by ISPs. *See* Supplemental TRO Exh. 1. Very briefly, the DNS poisoning method obstructs the most common process by which a computer converts a URL (like http://www.cdt.org) to a numeric IP address (such as 206.112.85.61),

---

[8] *See* AOL Dep. at 123-25 (describing AOL's null routing); Comcast Dep. at 24-26 (same); Epix/Basham Dep. at 11-14 (same); Verizon/Lebredo Dep. at 15-21 (same); Rule 30(b)(6) Deposition of WorldCom, Inc. (Craig Silliman), Sept. 24, 2003, submitted as Exhibit 14 (hereafter "WorldCom Dep."), at 95-98 (same).

[9] *See* AOL Dep. at 118-19 (DNS option not available to AOL; null routing only feasible option for AOL); *see also* WorldCom Dep. at 103-05 (null routing only feasible method).

[10] *See* Epix/Basham Dep. at 13-18 (describing DNS method); Verizon/Lebredo Dep. at 15-21 (same). One ISP, Epix, used both null routing *and* DNS poisoning in all cases. Following an instance of blocked content, however, Epix raised the problem to the Attorney General's office and was told that the ISP could from that point forward just use the DNS spoiling method. *See* Epix/Butchko-Krisa Dep. at 9-22.

which is necessary to reach the content located at www.cdt.org. The null routing method obstructs access to the web site by blocking access to the numeric IP address. Professor Marcus explains that the "null routing" of the IP address is the method that is more effective in terms of minimizing an ISP's risk of criminal liability.

Both technical methods of compliance can and have led to vast number of blocking of innocent web sites. Null routing, initially used by all five ISPs that have been deposed, can lead to blocking because of the prevalence of "shared IP addresses." Typically, many unrelated URLs can share the same numeric IP address, and when an ISP "null routes" an IP address, *all* web sites at that location on the Internet are blocked. In Paragraphs 40-53 of his Expert Report and Testimony, Professor Marcus explains the shared IP address scenario. *See id.* As Professor Marcus explains, the sharing of IP address is a very common practice, is effectively required for most "web hosting" companies, and is likely to increase in prevalence over the next few years.

The First Expert Report and Testimony of Michael B. Clark details certain research into the prevalence of shared IP addresses that Plaintiff CDT has conducted. *See* Supplemental TRO Exh. 2. The research reveals that of the almost 30 million web sites analyzed, over 90% share an IP address with at least one other web site, over 75% share with fifty other web sites, and almost 50% share with over five hundred other web sites. *See id.* ¶ 24.[11]

[11] Arguably, these percentages are mildly skewed by the fact that some IP addresses are used to "park" a high number of domain names with only minimal (but still constitutionally protected) content on them. For example, the evidence will show that the two most populated IP addresses (IP addresses 64.202.162.37 with 1,444,937 different domains, and 216.168.224.63 with 1,012,188 different domains, as of October 2002) appear to contain "parked" domains. But the third most populous IP address (216.21.229.209 with 716,158 different domains) contains many active, live web sites that are created by individual small businesses and other web publishers.

In any event, the report of Michael Clark reveals that even if one excludes all domains that share an IP address with more than 5,000 sites (which would exclude many web sites, including the great bulk of parked domains), still more than 75% of web sites share their IP address with more than 50 other web sites. Thus, even among web sites that have only a small amount of sharing, there is a very high level of IP address sharing.

Of the 600,000-plus web sites that Supplemental TRO Exhibit 15 indicates are blocked as a result of the Informal Notice process, all would be blocked by an ISP using the null routing method. The technical method disfavored by the ISPs (and wholly unavailable to AOL) – the DNS spoiling method – also creates a very high risk of blocking innocent content. Of the web sites listed in Supplemental TRO Exhibit 15, the 300,000-plus sites listed in Part D of that exhibit would be blocked by an ISP utilizing the DNS spoiling method. Although the likelihood that innocent content will be blocked with the DNS spoiling method is lower than with null routing method, the risk of blockage is substantial with either method.

From early in the Informal Notice process until most recently in this litigation, the Attorney General has asserted that DNS spoiling was the best method for ISPs to use. On December 5, 2003, for the first time (in the Defendants' expert report), the Defendant now appears to have abandoned both IP address null routing and DNS spoiling in favor of a proposed method – "URL filtering" – used by *none* of the ISPs. *See* Expert Report of Benjamin Stern (Dec. 5, 2003) (hereafter "Stern Report"). Plaintiffs believe that the evidence will show "URL filtering" to be what it is – a last-minute attempt to come up with a possible new method, now that the other two methods have been shown to block huge amounts of protected expression. This last-minute proposal is fatally flawed, but Plaintiffs' deposition of Defendant's expert witness has not yet taken place, and thus Plaintiffs have not yet completed their analysis of the problems with the "URL filtering" approach.

E. The Minimal Impact on the Child Pornography Business

Although the Informal Notices have led to extensive blocking of innocent web content, the Notices have almost certainly had negligible effect on curtailing the buying and selling of child pornography over the Internet. The Informal Notices have no direct effect whatsoever

against a seller or poster of child pornography, and only marginal indirect effect. Those individuals are allowed to continue operating with no interference by the Defendant.

Astoundingly, as the evidence will show, even when the Attorney General's office had (1) specifically identified a man in Ohio who posted child pornography on the Internet, and (2) directly communicated with the child pornographer, the Attorney General chose not to initiate or participate in any prosecution (by either Pennsylvania or Ohio authorities) of the perpetrator. Instead, the Attorney General simply sent an Informal Notice to the ISP, and allowed the child pornographer to remain free.

Equally important is the fact that the Informal Notices have very little effect on the users of child pornography (in Pennsylvania and elsewhere) who actively seek out the child pornography web sites that Defendant is seeking to block. Most such users of child pornography actively try to hide their online identity (to avoid investigation and prosecution by law enforcement officials), and the techniques used to hide identity (anonymizers and "anonymous proxy servers") *also work to completely circumvent* both technical methods (null routing and DNS spoiling) used by ISPs to comply with the Informal Notices (as well as the "URL filtering" proposed last week by Defendant's expert). In other words, a pedophile seeking to remain anonymous will be *unaffected* by an Informal Notice or an order under the Statute, even if at the same time the Informal Notices or orders block access to other, unrelated lawful web sites.

There are a number of places on the Internet where pedophiles and other consumers of child pornography congregate, and introductory documents, or "how to" guides, are available that offer advice to individuals who want to obtain child pornography. On December 2, 2003, Plaintiffs submitted to the Court, under seal, examples of the advice given to those interested in

child pornography. *See* Supplemental TRO Exh. 17 (under seal). Those documents specifically advise that individuals seeking child pornography use "anonymous proxy" services.

In his report at Paragraphs 68-73, Professor Marcus explains how anonymous proxy services work, and how those services completely circumvent the blocking methods used by the ISPs to comply with the Informal Notices. Supplemental TRO Exh. 1. The depositions of the ISPs confirmed this conclusion. *See, e.g.,* Comcast Dep. at 85-86; Rule 30(b)(6) Deposition of Verizon, Inc. (Richard Hiester), Oct. 3, 2003, excerpts in Supplemental TRO Exh. 13, at 35-41. Moreover, Michael Clark's Third Report (Supplemental TRO Exh. 4) demonstrates that the web site blocks imposed by AOL can be circumvented using a proxy service.

Thus, the Informal Notices have had only minimal effect on the ability of pedophiles and others in Pennsylvania who intentionally seek access to child pornography to obtain it online. At the same time they have resulted in the elimination of Internet users' access to well over one million lawful web sites, and continue to block access to at least 600,000 lawful sites.

F. The Proceedings to Date in this Case

On September 9, 2003, Plaintiffs sought a Temporary Restraining Order expressly limited to enjoining the issuance of additional Informal Notices. Immediately prior to the TRO hearing, the Defendant agreed to the requested relief, and the Court entered an order enjoining further Informal Notices. In Plaintiffs' Memorandum in support of their TRO motion, however, Plaintiffs stated:

> Plaintiffs also plan to seek preliminary injunctive relief against the statute itself and against the secret orders that the Attorney General has already issued, but first Plaintiffs seek focused and expedited discovery so that they can demonstrate to the Court, as soon as possible, the full breadth of innocent web sites that have been blocked.

Plaintiffs' Mem. in Support of TRO Motion at 2-3 (filed Sept. 9, 2003). The Court ordered that

expedited discovery take place, and Plaintiffs then aggressively sought to obtain sufficient facts from the Defendant, third party ISPs, and other sources to be able to identify some (but by no means all) of the unrelated web sites blocked as a result of the hundreds of Informal Notices issued by Defendant over the past eighteen months. Only in the last half of November did Plaintiffs finally have sufficient information to identify blocked sites, and Plaintiffs then returned to Court on December 2, 2003, to seek additional TRO and/or preliminary injunctive relief against the existing Informal Notices and against the use of the Statute. As a result of that motion, the parties held a teleconference with the Court on December 4, 2003, during which it was agreed that Plaintiffs would submit a superseding Motion for Preliminary and Permanent Injunctive Relief and supporting Memorandum, which would be heard by the Court on January 6, 2004. This is that Memorandum.

SUMMARY OF ARGUMENT

In support of their motion, Plaintiffs set out the following factual and legal arguments:

The blocking by ISPs of access to specified Internet web sites, as required by both the Informal Notices and the Statute, has led to vast and continuing interference with constitutionally protected speech on the Internet.

The very theory of the Informal Notices and the Statute – which have the effect of preventing *all* speech, without regard to its content, at a particular location on the Internet – represents a classic prior restraint and it wholly unsupportable under clear First Amendment law.

Well-established First Amendment jurisprudence indisputably demonstrates that the government cannot suppress protected expression in an effort to attack unprotected expression, especially on the scale that has occurred here.

The procedures (or lack thereof) of the Informal Notices and the Statute fall far short of the constitutional minimums set by the Supreme Court, and alone these procedural defects require a judgment for Plaintiffs in this case.

The Informal Notices and the Statute violate the Commerce Clause because they inevitably impose restrictions on communications wholly outside Pennsylvania,

impermissibly burden interstate commerce and create a risk that speech on the Internet will be subject to inconsistent state obligations.

The unprecedented scale of curtailed speech at issue here, when combined with the overwhelming weight of First Amendment, Fourteenth Amendment and Commerce Clause analysis, establish an unusually strong case that both the Informal Notices and the Statute should be permanently enjoined.

ARGUMENT

Section I addresses the question of the Plaintiffs' standing. Section II analyzes the fundamental constitutional problems raised by the novel approach taken in both the Statute and the Informal Notices – the attempt to regulate Internet content by blocking access to URLs and IP addresses on the Internet. Sections III and IV look at the First and Fourteenth Amendment issues raised by the Statute and the Informal Notices, respectively. Finally, Section V addresses the Commerce Clause problems raised by both the Statute and the Informal Notices. In a telephone conference in early December, the Court asked whether the First Amendment standards governing efforts to regulate child pornography differ from those applicable to efforts to regulate obscenity; that issue is directly addressed in Section III.C below.

To the extent this Court treats Plaintiffs' motion as one for preliminary relief, Plaintiffs clearly meet the four-part test for a preliminary injunction. *See* Plaintiffs' Mem. in Support of TRO Motion (filed Sept. 9, 2003); Plaintiffs' Mem. in Support of Supplemental TRO Motion (filed Dec. 2, 2003).

I. THE PLAINTIFFS HAVE STANDING TO SEEK DECLARATORY AND INJUNCTIVE RELIEF.

The Statute and Informal Notices before the Court are challenged by two sets of Plaintiffs. Each has demonstrated the requisites of Article III standing: injury in fact, causation, and redressability. *See, e.g., Friends of the Earth, Inc. v. Laidlaw Envtl. Servs., Inc.*, 528 U.S. 167, 180-81 (2000).

First, Plaintiff Plantagenet, Inc., a Pennsylvania ISP, seeks to prevent the Defendant in the future from invoking against it either the Informal Notice system previously deployed against other ISPs, or the more formal apparatus made available by the Statute. It seeks a declaration that these practices and the Statute are unconstitutional, and an injunction against future impositions. The prospect of becoming enmeshed in a state's criminal enforcement machinery directed against constitutionally protected conduct is a classic injury in fact that vouchsafes standing in federal court. *See, e.g., Virginia v. American Booksellers Ass'n, Inc.*, 484 U.S. 383, 392-93 (1988) (pre-enforcement challenge is properly entertained where "the State has not suggested that the newly enacted law will not be enforced" and plaintiffs have alleged they would be forced to take costly compliance measures or risk criminal prosecution); *cf. Stenberg v. Carhart*, 530 U.S. 914, 945 (2000) ("using this law some present prosecutors and future Attorneys General may choose to pursue physicians. . . . All those who perform abortion procedures using that method must fear prosecution, conviction, and imprisonment"); *New Hampshire Right to Life Political Action Comm. v. Gardner*, 99 F.3d 8, 14 (1st Cir. 1996) ("The standard – encapsulated in the phrase 'credible threat of prosecution' – is quite forgiving.").

This is particularly true where, as here, the statutory scheme has already been invoked against the speech of other similarly situated entities. *See, e.g., City of Houston v. Hill*, 482 U.S. 451, 459, n.7 (1987) (finding standing where there is "a genuine threat of enforcement" against

future speech); *Steffel v. Thompson*, 415 U.S. 452, 459 (1974). As the Third Circuit recently observed in *Planned Parenthood of Central N.J. v. Farmer,* 220 F.3d 127,148 (3d Cir. 2000):

> "[w]hen the plaintiff has alleged an intention to engage in a course of conduct arguably affected with a constitutional interest, but proscribed by a statute, and there exists a credible threat of prosecution thereunder, he 'should not be required to await and undergo a criminal prosecution as the sole means of seeking relief.'" *Babbitt v. United Farm Workers Nat'l Union*, 442 U.S. 289, 298 (1979) (citation omitted). . . . The Act fairly easily can be read to prohibit those constitutionally protected procedures [in which the plaintiffs have engaged], and plaintiffs received no assurances that it would not be enforced against them if they performed such procedures. They were entitled to know what they could not do."

See also ACLU v. Ashcroft, 322 F.3d 240, 266 n.33 (3d Cir. 2003), *cert. granted,* 124 S. Ct. 399 (2003) (holding plaintiffs apparently covered by statute had standing to bring pre-enforcement challenge even where potential prosecutors claimed that statute did not apply).

In addition to having a constitutionally cognizable interest in being free of the Defendant's statutory or informal order system, Plaintiff Plantagenet also has a protected interest in being able to offer to its customers the broadest possible range of lawful content available on the Internet. *See Turner Broad. Sys., Inc. v. FCC.*, 512 U.S. 622, 636-37 (1994) (cable service provider has First Amendment interest in control over what content it can offer). Finally, Plantagenet has brought this action on behalf of its customers, and like Plaintiff ACLU (discussed below), Plantagenet can advance the constitutional interests of those customers.

The second set of Plaintiffs consists of (1) the Center for Democracy and Technology ("CDT"), which obtains its Internet access from WorldCom, an ISP that has been directly subject to orders under both the Informal Notice system and the Statute, and (2) the American Civil Liberties Union of Pennsylvania ("ACLU"), which brings this action on behalf of its members whose ISPs have been subject to informal blocking orders, and which may again be subject to

either formal or informal orders in the future.[12] These Plaintiffs are prepared to prove that the enforcement of the formal statutory scheme will do what the challenged informal orders have already done: place obstacles in the path of their right to receive information from innocent and lawful websites, and burden access to the "vast democratic forum of the Internet," *Reno v. ACLU*, 521 U.S. 844, 853, 868 (1997), by preventing their ISPs from providing untrammeled access to subscribers in Pennsylvania.

It is a well-settled principle of constitutional law that the First Amendment protects not only the speaker's right to convey information, but also the listener's right to receive the

---

[12] The ACLU's right and ability to represent the interests of its members is clear. Under well-settled Supreme Court and Third Circuit law, a membership organization has standing to challenge a government action on behalf of its members when (1) those members themselves would have standing to sue in their own right, (2) the interests protected are germane to the organization's purpose, and (3) neither the claim nor the relief requires the participation of individual members. *See, e.g., Friends of the Earth*, 528 U.S. at 181; *United Food & Commercial Workers Union Local 751 v. Brown Group, Inc.,* 517 U.S. 544 (1996); *Hunt v. Washington State Apple Adver. Comm'n*, 432 U.S. 333, 343 (1977); *Sierra Club v. Morton*, 405 U.S. 727, 739 (1972); *Freethought Soc'y v. Chester County*, 334 F.3d 247, 255 n.3 (3d Cir. 2003); *Pennsylvania Psychiatric Soc'y v. Green Spring Health Servs.*, 280 F.3d 278 (3d Cir.), *cert. denied*, 537 U.S 881 (2002). Of particular relevance is *Virginia Pharmacy Board v. Virginia Citizens Consumer Council*, 425 U.S. 748, 754 n.10 (1976) (consumer organizations can challenge ban on advertising by pharmacists; each organization "has a substantial membership . . . many of whom are users of prescription drugs).

Applying this standard, federal courts have repeatedly permitted the ACLU to vindicate the constitutional rights of its members. *See, e.g., County of Allegheny v. ACLU Greater Pittsburgh Chapter*, 492 U.S. 573 (1989); *ACLU of N.J. v. Schundler*, 168 F.3d 92 (3d Cir. 1999), *ACLU of Ill. v. City of St. Charles*, 794 F.2d 265, 267 (7th Cir. 1986) ("since the American Civil Liberties Union alleges no injury to itself, its standing depends on that of its members, the individual plaintiffs") (citation omitted); *see also J-R Distribs. v. Eikenberry*, 725 F.2d 482, 485 n.2 (9th Cir. 1984) (in challenges brought to Washington's anti-obscenity statute, the court stated "it is worth noting however that the ACLU has standing to sue in this case if any one of its members suffers or is threatened with injuries that would create justiciable case . . . . Because we find that [the statute] is unconstitutionally overbroad it seems likely that some of the ACLU's members would be affected by the statute's impermissible restrictions on protected speech"). In this case Plaintiffs will submit to the Court the verifications of Clark Moeller, Gene Bishop, Janet Goldwater, and Dana Devon, each of whom are members of the ACLU as well as active participants in the work of chapter and state ACLU boards. In turn, these individuals secure Internet access through the following service providers: Epix.net, AOL, Verizon, and Comcast, all of which have received scores of Informal Notices. Each of these individuals further state that they have occasion to utilize the "Google.com" search engine to retrieve information maintained on various websites, the existence of which they have no prior knowledge. In light of that fact, each needs to have access to the broadest reaches of the Internet. As a result of the over-blocking that results from both the Statute and the Defendant's Informal Notices, these ACLU members have been denied, and will continue to be denied, access to hundreds of thousands of web sites on the Internet. This denial of access to constitutionally protected information constitutes a legally cognizable injury. *See Kleindienst v. Mandel*, 408 U.S. 753, 762

information. *See, e.g., Board. of Educ. v. PICO*, 457 U.S. 853, 867 (1982); *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 576 (1980); *Kleindienst v. Mandel*, 408 U.S. 753, 762-65 (1972); *Red Lion Broad. Co. v. FCC.*, 395 U.S. 367, 390 (1969); *Stanley v. Georgia*, 394 U.S. 557, 564 (1969); *Lamont v. Postmaster General*, 381 U.S. 301 (1965); *Martin v City of Struthers*, 319 U.S. 141, 143 (1943). As Justice Brennan observed,"[t]he dissemination of ideas can accomplish nothing if otherwise willing addressees are not free to receive and consider them. It would be a barren marketplace of ideas that had only sellers and no buyers." *Lamont*, 381 U.S. at 308 (Brennan, J., concurring).

The Supreme Court has recognized that this principle applies with full force to the Internet. In *Reno v. ACLU*, 521 U.S. at 874, the Court invalidated the Communications Decency Act because "in order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive." *See also United States v. American Library Ass'n*, 123 S. Ct. 2297, 2310 (2003) (Breyer, J., concurring in the judgment) ("The Constitution protects the right to receive information and ideas") (quoting *Stanley v. Georgia*, 394 U.S. at 564).

The infringement of the rights of the CDT and ACLU plaintiffs (as well as Plantagenet's customers) to receive information blocked by the challenged scheme is itself a cognizable injury in fact that will be redressed by the relief Plaintiffs request. It is of no consequence to the standing of the Plaintiffs that the mechanism of this infringement is a regulation directed at their ISPs. Both the Supreme Court and the Third Circuit have regularly entertained cases where the plaintiffs' claims of injury have consisted of interference with their right to obtain information by virtue of the interference of third parties with the transmission of information by willing

---

(1972) ("in a variety of contexts this Court has referred to a First amendment right to 'receive information and ideas'").

speakers. *See, e.g., Board of Educ. v. PICO*, 457 U.S. at 867 (students have standing to challenge removal of books from school library); *Kleindienst*, 408 U.S. at 762-65 (in furtherance of their own right to receive information and ideas, professors could challenge exclusion by immigration authorities of Belgian who was invited to speak at professors' conference); *FOCUS v. Allegheny County Court of Common Pleas*, 75 F.3d 834 (3d Cir. 1996) (third party citizens advocacy group challenged gag order imposed on parties to litigation; "putative recipients of speech usually have standing to challenge orders silencing would-be speakers"); *New Jersey-Philadelphia Presbytery of the Bible Presbyterian Church v. New Jersey State Bd. of Higher Educ.*, 654 F.2d 868 (3d Cir. 1981) (students had standing to challenge state regulation that interfered with communications from their teachers). *See also Federal Election Comm'n v. Akins*, 524 U.S. 11, 21-25 (1998) (citizens group had standing to challenge regulator's refusal to order third party to publish information); *Vasquez v. Housing Auth. of El Paso*, 271 F.3d 198 (5th Cir. 2001) (resident of housing project had standing to challenge enforcement of trespassing regulation against candidates from outside the housing project involved in door-to-door circulation).

The most directly relevant example is *Virginia Pharmacy Board v. Virginia Citizens Consumer Council, Inc.*, 425 U.S. 748, 756 (1976), where the Supreme Court granted relief in an action by prescription drug consumers challenging ban on advertising by pharmacists. Just as the enforcement of the advertising ban against pharmacists deprived consumers of the information that pharmacists would otherwise convey, so too here the orders issued against their ISPs block access to information to which the Plaintiffs are constitutionally entitled. *See ACLU v. Ashcroft*, 322 F.3d at 266 n.33 (approving Eastern District of Pennsylvania holding that

organization had "listener" standing as user of Web to challenge statute requiring web posters to impose burdens on access).

Having established that they have standing to assert their own (and their customers' and members') First Amendment rights to receive information, Plaintiffs are entitled as well to bring before the Court the correlative rights of speakers to convey information, and the rights of other listeners also affected by the challenged scheme. The Supreme Court has held that the important function of preventing suppression of speech allows plaintiffs challenging an overbroad statute to raise before the courts the legal rights of absent parties affected by that statute who may themselves be unable or unwilling to bring challenges. As the Court set forth the doctrine in *Virginia v. American Booksellers Ass'n*:

> [I]n the First Amendment context, [l]itigants . . . are permitted to challenge a statute not because their own rights of free expression are violated, but because of a judicial prediction or assumption that the statute's very existence may cause others not before the court to refrain from constitutionally protected speech or expression.

484 U.S. at 392-93 (internal quotation marks and citation omitted).[13] In *American Booksellers*, the Court allowed the plaintiff book store owners to raise the rights of prospective adult customers to unfettered access to books that might be deemed "harmful to minors" without burdensome limits on display of such works.[14] So too, here, plaintiffs may raise the rights of the

[13] *See also Secretary of State of Md. v. J.H. Munson Co.*, 467 U.S. 947, 957 n.5 (1984) ("[I]n First Amendment cases we have relaxed our rules of standing without regard to the relationship between the litigant and those whose rights he seeks to assert precisely because application of those rules would have an intolerable, inhibitory effect on freedom of speech") (quoting *Eisenstadt v. Baird*, 405 U.S. 438, 445 (1972); *Forsyth County v. Nationalist Movement*, 505 U.S. 123, 129 (1992) ("the very existence of some broadly written laws has the potential to chill the expressive activities of others not before the court"); *Village of Schaumburg v. Citizens for a Better Environment*, 444 U.S. 620, 634 (1980) ("Given a case or controversy, a litigant whose own activities are unprotected may nevertheless challenge a statute by showing that it substantially abridges the First Amendment rights of other parties not before the court."). The Third Circuit has recently expressly confirmed this relaxed standards for standing in overbreadth cases in its decision on the federal Child Online Protection Act. *See ACLU v. Ashcroft*, 322 F.3d at 266 n.33.

[14] The Supreme Court has regularly considered the rights of willing listeners when those rights are raised by speakers whose actions are inhibited. *See, e.g., Reno v. ACLU*, 521 U.S. at 875 (in evaluating claims of

hundreds of thousands of owners of innocent and lawful websites whose access to their audience, and the similar number of web surfers whose access to those web sites, is burdened by the statutory and informal schemes of censorship at issue.

The need to permit Plaintiffs to raise the rights of speakers is especially acute here, where the affected speakers and listeners have no way of knowing that the transmission of messages to willing recipients has been covertly blocked, and even if they are aware of the blocking may not have the resources to challenge the government's actions. If the rights of these speakers and other listeners are not raised by the Plaintiffs, those rights will go unvindicated.

II. THIS CASE REPRESENTS THE FIRST APPLICATION OF WELL-ESTABLISHED PRIOR RESTRAINT DOCTRINE TO INTERNET URLS AND IP ADDRESSES, AND THAT DOCTRINE REQUIRES A FINDING THAT BOTH THE STATUTE AND THE INFORMAL NOTICES ARE UNCONSTITUTIONAL.

In *ACLU v. Reno*, 929 F. Supp. 824 (E.D. Pa. 1996), a three-judge panel of the Eastern District of Pennsylvania declared that the Internet should receive the fullest protection under the First Amendment, and that holding was fully upheld by the Supreme Court in *Reno v. ACLU,* 521 U. S. 844 (1997). Following the mandate of *Reno v. ACLU*, courts have applied long-standing First Amendment jurisprudence from the off-line world to evaluate issues arising in the online world. The instant case, however, goes beyond prior cases to ask the Court to determine (for the first time, as far as Plaintiffs are aware) how that off-line jurisprudence should be applied to governmental actions aimed at the specific and very technical naming and addressing systems

---

speakers courts must weigh the rights of potential listeners; government may not "reduce the adult population . . . to . . . only what is fit for children"); *Martin v. Struthers*, 319 U.S. at 147, 149 (First Amendment freedom "embraces the right to distribute literature, and necessarily protects the right to receive it. . . . Freedom to distribute information to every citizen whenever he desires to receive it is so clearly vital to the preservation of a free society that, putting aside reasonable police and health regulations of time and manner of distribution, it must be fully preserved."). Listeners whose rights are violated should similarly be able to raise the constitutional interests of speakers.

used by most communications on the Internet. The resolution of this question is likely to determine whether the Internet will continue to be the robust, open and democratic mode of communications that it is today, or whether instead governments will be able to force ISPs to act as censoring bottlenecks through which all Internet communications must pass.

In the off-line world, the First Amendment has commonly allowed two types of legal attack on pornographic material – actions against a person for past distribution of specific pornographic content, and actions against one or more specific instances of such content. Thus, criminal charges can be brought against individuals accused of distributing specific items of content alleged to be obscene or child pornography. Similarly, cases can directly target (usually for seizure) one or more specific items alleged to be obscene or child pornography. *See, e.g., United States v. 12 200-FT. Reels of Super 8mm Film*, 413 U.S. 123 (1973). When the target of governmental action moves beyond those two common scenarios, however, far greater First Amendment concerns have historically been implicated. When government attempts to prohibit future speech either in a particularly named publication or in a particular location, the long line of prior restraint cases discussed below are implicated. *See Near v. Minnesota ex rel. Olson*, 283 U.S. 697 (1931); *Organization for a Better Austin v. Keefe*, 402 U.S. 415 (1971); *Vance v. Universal Amusement Co., Inc.*, 445 U.S. 308 (1980).

In this case, the Statute and the Informal Notices bypass the common and constitutionally accepted approaches to targeting pornographic speech, and instead use a novel technical approach that runs squarely into the classic prior restraint cases. Here, the Defendant has taken no action against the perpetrators of the child pornography (either the creators or the posters). Nor, critically, has the Defendant sought to seize or restrain any specific and static pieces of expressive material. Instead, the Defendant is in essence seeking to impose an absolute and

never-ending bar on *all* expression of any sort that might in the future take place at the specific URLs or IP addresses that are affected by the Informal Notices and orders under the Statute.

In other words, rather than criminalizing an individual's conduct, or declaring that a specific piece of expressive material is illegal contraband, the Defendant and the Statute seek to criminalize a *location* at which illegal content was in the past found. To give a concrete example, because the Defendant believed that content located in June 2002 at "www.RedactedURL1.com" contained child pornography, the Defendant issued Informal Notice 1537 to America Online, Inc. (AOL) seeking to permanently prevent access to any speech of any kind, at any point in the future, at the Internet location "www.RedactedURL1.com." Specifically, Defendant's order to AOL required that "[a]ccess to uniform resources locator www.RedactedURL1.com be denied to your subscribers to your services from an address located within the Commonwealth of Pennsylvania." *See* TRO Exh. 1. The practical effect of this Informal Notice, as implemented by AOL, is that the Defendant has permanently prevented access to any speech of any kind, at any point in the future, at the location designated by IP address 209.25.162.15. For the two ISPs (Verizon and Epix) that also use the "DNS spoiling" method to comply with an Informal Notice, the ISP is permanently preventing access to any speech of any kind, at any point in the future, at the location designated by the URL.

Under both the Informal Notice system and the Statute, the Attorney General is able to impose a permanent, never-to-be-reviewed prohibition preventing speech of any kind from taking place at a certain *location* on the Internet. To translate this to the physical, off-line world, it would be as if the government entered an order that because (1) a movie theater at 123 Market Street showed an obscene movie in June 2002, then (2) no speech of *any* kind can take place in the future at 123 Market Street. No lawful movies could be shown at that location, and indeed,

no newspaper or TV station could tear down the theater and begin to operate at 123 Market Street. Under the approach taken by the Statute and the Informal Notices, 123 Market Street would become permanently off-limits for all forms of speech for an unlimited period of time.

In considering the Statute and the Informal Notices, it is important to recognize that a URL is in fact merely a location at which content (or non-content oriented services) on the Internet might be found. It is not, to be sure, a physical location like 123 Market Street, but both Uniform Resource *Locators* and IP *addresses* are cyberspace equivalents to physical world locations. And, taken alone, the strings of letters and numbers that make up URLs and IP addresses (such as URL www.RedactedURL1.com or IP address 209.25.162.15) are not themselves obscene or child pornography.[15]

It is in this context – that the Statute and the Informal Notices both expressly target Internet locations in the form of URLs, and that many ISPs carry out the orders by blocking another type of Internet location, IP addresses – that the Supreme Court's prior restraint jurisprudence must be applied. The seminal prior restraint case is *Near v. Minnesota ex rel. Olson*, 283 U.S. 697 (1931), which although pre-dating the Internet by more than 50 years is nevertheless directly applicable to the case now before this Court. In that case, Mr. Near and his colleagues published a weekly periodical called *The Saturday Press*, which the county attorney alleged (apparently with some degree of accuracy) was filled with articles "largely devoted to malicious, scandalous and defamatory articles" concerning a number of local public officials. *Id.* at 703. Under a state nuisance statute, the county attorney obtained a court order to enjoin the publication or circulation of "'any future editions of said *The Saturday Press*.'" *Id.* at 705. The

[15] Indeed, the letters that make up "www.RedactedURL1.com" are not even suggestive of child pornography. Even URLs that reference "lolita" or other words that suggest child pornography cannot alone be viewed as illegal content under the First Amendment. Moreover, the Pennsylvania law itself only criminalizes *images* as child pornography, not text that hints at child pornography. 18 Pa. Stat. Ann. § 6312.

U.S. Supreme Court concluded that even if past issues of *The Saturday Press* had been illegal under state libel laws (something the Court effectively assumed might be true), the prospective suppression of future editions of the publication "is of the essence of censorship" and must be overturned. *Id*. at 713, 723.

When in the early 1930s Mr. Near was publishing what amounted to personal diatribes against what he viewed as a conspiracy between "Jewish gangsters" and public officials, *id*. at 704, few people could afford to distribute widely such personal and antagonistic views. It does not take much imagination, however, to conclude that if Mr. Near wanted to air his views today – in 2003 – that his publication would almost certainly be located at "www.TheSaturdayPress.com" on the Internet, and the court order at issue in the *Near* case would have likely been phrased as enjoining the publication of "any future editions of said *www.TheSaturdayPress.com*."[16] Just as the Supreme Court struck down the prior restraint of future editions of *The Saturday Press*, the First Amendment today cannot countenance the perpetual prohibition of speech at any particular URL on the Internet.[17]

The direct applicability of prior restraint cases from the off-line world to the Internet is seen even more strikingly in the U.S. Supreme Court's 1980 decision in *Vance v. Universal Amusement Co., Inc.*, 445 U.S. 308 (1980). In that case, the Supreme Court reviewed a Texas statute that is remarkably analogous to the Statute challenged here. The law allowed state court

[16] If one views a URL as less of a "location" and more of a title of a publication, the holding of *Near* continues to apply with equal force. In the Internet context, the URL www.RedactedURL1.com could simply be viewed as the title of a publication (instead of the location of a publication). The *Near* case makes clear that a publication named "www.RedactedURL1.com" cannot be prospectively enjoined, while the *Vance* case discussed below makes clear that communications located at www.RedactedURL1.com (or at IP address 209.25.162.15) cannot be prospectively enjoined.

[17] Indeed, as discussed in Sections III.B and IV.A below, the case before the Court today is more problematic than in *Near*. In *Near*, the actual publisher of the challenged content was given prior notice and an opportunity to fight the censoring injunction. In this case, the publisher of the challenged web sites are not even informed of the censorship, much less given a chance to respond or defend their web sites.

judges, in an *ex parte* proceeding and on the basis of a showing that a movie theater exhibited obscene films in the past, to enjoin any future exhibition of movies not yet found to be obscene. *Id*. at 308, 312. The Court characterized the Texas law as "authorizing a prior restraint of indefinite duration on the exhibition of motion pictures without a final judicial determination of obscenity and without any guarantee of prompt review of a preliminary finding of probable obscenity." *Id*. at 309; *see also id*. at 316. The Supreme Court had no difficulty finding the prospective restraint on the future display of unidentified (and indeed unknowable) future content could not pass First Amendment scrutiny. *See id*. at 317.

The result rejected in *Vance* is *exactly* the result obtained by both the Statute and the Informal Notices. As a result of the orders challenged in this litigation, speech of any kind simply cannot take place on certain identified locations on the Internet. As in *Vance*, this type of prospective censorship of speech at a particular location cannot withstand First Amendment review.[18]

To make its holding in *Vance* unmistakably clear, the Supreme Court declared that "the burden of supporting an injunction against a future exhibition is even heavier than the burden of justifying the imposition of criminal sanction for a past communication." *Id*. at 316. In a footnote, the Court expanded on this holding:

> The presumption against prior restraints is heavier – and the degree of protection broader – than that against limits on expression imposed by criminal penalties. Behind the distinction is a theory deeply etched in our law: a free society prefers to punish the few who abuse rights of speech after they break the law than to throttle them and all others beforehand.

Id. at 316 n.13. As has been made plainly clear in discovery in this case, the risk of throttling "all others" through prior restraints is serious.

[18] *See also Organization for a Better Austin v. Keefe*, 402 U.S. at 419 (overturning as an unconstitutional prior restraint an injunction barring the distribution of literature "of any kind" in an entire city of 18,000 people).

Under both *Near* and *Vance*, the fundamental theory that underlies both the Statute and the Informal Notices must fail. The Statute and the Informal Notices both fail to target either the perpetrators of the child pornography or the child pornography itself. Instead, both the Statute and the Informal Notices single out specific URLs and require that access to those URLs be blocked.[19] By seeking to enjoin permanently access to any content that may in the future be available on specific URLs (and specific IP addresses by way of the compliance methods of many ISPs), both the Statute and the Informal Notices create unconstitutional prior restraints under *Near* and *Vance*.

[19] The concern about prior restraints targeted specifically at URLs is heightened by the possibility that URLs themselves, standing alone, may be protected expression. In trademark and other litigations, some courts have held that URLs, by themselves, are protected expression under the First Amendment. *See, e.g., Taubman Co. v. Webfeats*, 319 F.3d 770, 778 (6th Cir. 2003) (finding in that case that "the domain name is a type of public expression, no different in scope than a billboard or a pulpit"); *Bally Total Fitness Holding Corp. v. Faber*, 29 F. Supp. 2d 1161, 1167 (C.D. Cal. 1998) (holding that URL "www.compupix.com/ballysucks" is "speech protected by the First Amendment"). In *Name.Space, Inc. v. Network Solutions, Inc.*, 202 F.3d 573 (2d Cir. 2000), the Second Circuit considered whether a three-letter "top level domain" (TLD) such as ".com" or ".net" could alone be protected expression. In concluding that three-letter TLDs are not protected, that court made clear that a longer TLD (and, in Plaintiffs' view, *a fortiori* a full URL) could well be protected expression:

> [T]he functionality of domain names does not automatically place them beyond the reach of the First Amendment. Although domain names do have a functional purpose, whether the mix of functionality and expression is "sufficiently imbued with the elements of communication" depends on the domain name in question, the intentions of the registrant, the contents of the website, and the technical protocols that govern the DNS. . . . Functionality and expression are therefore not mutually exclusive: for example, automobile license plates have a functional purpose, but that function can be served as well by vanity plates, which in a small way can also be expressive. Similarly, domain names may be employed for a variety of communicative purposes with both functional and expressive elements, ranging from the truly mundane street address or telephone number-like identification of the specific business that is operating the website, to commercial speech and even core political speech squarely implicating First Amendment concerns.

Id. at 585-86 (citation and footnote omitted). In this case, none of Plaintiffs' claims turn on or require a holding that URLs, taken alone, are protected expression under the First Amendment. The fact, however, that a growing number of courts have found URLs to be protected speech should confirm the need to apply the full array of searching substantive and procedural First Amendment analyses to the claims raised by Plaintiffs in this case.

III. THE STATUTE MUST BE PERMANENTLY ENJOINED UNDER BOTH THE FIRST AND FOURTEENTH AMENDMENTS.

A. The Statute is Unconstitutional Under Traditional First Amendment Analysis.

In addition its unconstitutional banning of certain URLs and IP addresses, this case presents a quintessential First Amendment violation with regard to Internet content, both under the overbreadth doctrine and strict scrutiny. Because of the technical architecture of the Internet, implementation of the Pennsylvania Statute has resulted in the blocking of more than one million web sites – web sites that *no one* has argued contain unprotected speech. Although "the objective [of the law] is to prohibit illegal conduct, [the] restriction goes well beyond that interest by restricting the speech available to law-abiding adults." *Ashcroft v. Free Speech Coalition*, 535 U.S. 234, 252-53 (2002). In the face of long-established First Amendment doctrine, this sweeping censorship of entirely legal, protected speech cannot stand.

1. The Statute is Unconstitutionally Overbroad.

As a threshold matter, the Statute must be enjoined as unconstitutionally overbroad. "The Government may not suppress lawful speech as the means to suppress unlawful speech," *Free Speech Coalition*, 535 U.S. at 255, yet that is precisely what Pennsylvania has done.

Under the substantial overbreadth doctrine, a law must be struck down as facially invalid if it would " 'penalize a substantial amount of speech that is constitutionally protected' . . . even if some applications would be 'constitutionally unobjectionable.'" *ACLU v. Reno*, 929 F. Supp. at 867 (opinion of Dalzell, J.) (quoting *Forsyth County v. Nationalist Movement*, 505 U.S. 123, 129-30 (1992)); *see also Free Speech Coalition*, 535 U.S. at 244 (a statute "is unconstitutional on its face if it prohibits a substantial amount of protected expression"); *ACLU v. Ashcroft*, 322 F.3d

at 266-67. Courts have not hesitated to find statutes facially invalid where technological limitations have caused the impact on protected speech. For example, in *Reno v. ACLU*, the Supreme Court struck down the Communications Decency Act because "existing technology did not include any effective method for a sender to prevent minors from obtaining access to its communications on the Internet without also denying [legal] access to adults." 521 U.S. at 876. Likewise here, existing technology does not allow ISPs to block access to any single URL without also denying their customers access to other legal URLs sharing an IP address with the targeted web site, and this technological reality has already resulted in the blocking of more than one million innocent web sites.

The magnitude and certainty of the censorship of protected speech in this case are unprecedented. Indeed, although this case differs from the standard overbreadth challenge, it does so for reasons that make it unusually obvious that the Statute is unconstitutional. In most overbreadth cases, the overbreadth effect is "at best a prediction." *Broadrick v. Oklahoma*, 413 U.S. 601, 615 (1973)). Thus, to ensure there is a serious threat to First Amendment rights before a statute is facially invalidated, the predicted overbreadth "'must not only be real, but substantial as well, judged in relation to the statute's plainly legitimate sweep.'" *New York v. Ferber*, 458 U.S. 747, 770 (1982) (quoting *Broadrick*, 413 U.S. at 615). Here, there is no need to rely on a mere prediction of overbreadth; we know with certainty that the Informal Notices based on the Statute have resulted in the blocking of more than one million web sites, and that further implementation of the Statute would have similar results. Indeed, it would be a striking understatement to say that the Statute burdens a "substantial" amount of constitutionally protected speech. The Statute is not only "*susceptible* of regular application to protected expression," *City of Houston v. Hill*, 482 U.S. at 467 (emphasis added); given the existing state

of technology, it is certain to be so applied. *A fortiori*, it is fatally overbroad, and therefore "facially invalid." *Id.*

2. The Statute is Content-Based and Thus Strict Scrutiny Applies.

As a content-based regulation of speech, the Statute also fails under a strict scrutiny analysis. Prohibitions and other regulations of child pornography and obscenity are "unabashedly content-based laws." *Ferber*, 458 U.S. at 756; *see also id.* at 763. Like the Pennsylvania Statute, such laws are "not justified without reference to the content of the regulated speech." *United States v. Playboy Entertainment Group, Inc.*, 529 U.S. 803, 811 (2000) (citation and internal quotation marks omitted). The proper analysis therefore starts with the presumption that the Statute's content-based restrictions on speech are "beyond the power of the government." *Simon & Schuster v. Members of New York State Crime Victims Bd.*, 502 U.S. 105, 115-16 (1991); *see also Playboy Entertainment,* 529 U.S. at 817 ("Content-based regulations are presumptively invalid") (quoting *R.A.V. v. St. Paul*, 505 U.S. 377, 382 (1992)).

Such content-based regulations of speech are subject to strict scrutiny, which means they are constitutionally permissible only when they are both justified by compelling governmental interests and "narrowly tailored" to effectuate those interests. *See Playboy Entertainment,* 529 U.S. at 813; *ACLU v. Ashcroft*, 322 F.3d at 251-66 (applying strict scrutiny to Internet obscenity statute); *Fabulous Assocs. Inc., v. Pennsylvania Pub. Util. Comm'n*, 896 F.2d 780, 788 (3d Cir. 1990) (applying strict scrutiny to strike down "harmful to minors" restrictions in telephone communications because of the unconstitutional burden on adult rights). In concluding that strict scrutiny applies equally to content-based bans on *Internet* speech, the Supreme Court has affirmed that there is "no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium." *Reno v. ACLU*, 521 U.S. at 870. *See also id.* at 874 ("Th[e] burden

on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve."). Thus, the Statute at issue here must be struck down unless the Attorney General demonstrates it serves a compelling interest, and that it does so "by narrowly drawn regulations designed to serve those interests without unnecessarily interfering with First Amendment freedoms." *Sable Communications of Cal., Inc. v. FCC*, 492 U.S. 115, 126 (1989).

Moreover, the burden is squarely on the government to prove the constitutionality of the Statute. *See Playboy Entertainment*, 529 U.S. at 816-17 (citing long line of Supreme Court cases). It is in this case the Defendant's burden to establish both that the Statute would in fact substantially further the governmental objective, and that the Statute is the least restrictive means to further that objective.

A straightforward application of these settled principles invalidates the Statute, for two reasons. First, the burden imposed by the Statute's restrictions is so severe in relation to the marginal gains in combating child pornography achieved by the law that it must be struck down. Second, the government cannot meet its heavy burden of proving that the Statute directly advances the compelling interest of combating child pornography in the least restrictive way.

3. Although There is a Compelling Government Interest, It is Not Significantly Furthered by the Statute.

The stated goal of the Statute, to combat child pornography, is without question a compelling government interest. But under strict (and even intermediate) scrutiny, a law "'may not be sustained if it provides only ineffective or remote support for the government's purpose,'" *Edenfield v. Fane*, 507 U.S. 761, 770 (1993) (quoting *Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n*, 447 U.S. 557, 564 (1980)), or if there is "little chance" that the restriction

will advance the State's goal, *Lorillard Tobacco Co. v. Reilly*, 533 U.S. 525, 566 (2001) (quoting *Greater New Orleans Broad. Ass'n v. United States*, 527 U.S. 173, 193 (1999)).

The government bears the burden of showing that its scheme will in fact alleviate the alleged "harms in a *direct and material* way." *Turner,* 512 U.S. at 624 (emphasis added). Here, the Defendant cannot meet his burden. As Justice Scalia wrote in his concurrence in *Florida Star v. B.J.F.*, 491 U.S. 524, 541-42 (1989), "a law cannot be regarded as . . . justifying a restriction upon truthful speech, when it leaves appreciable damage to [the government's] supposedly vital interest unprohibited." *Id.* at 541-42 (Scalia, J., concurring). *See, e.g., FCC v. League of Women Voters of Cal.*, 468 U.S. 364, 396 (1984) (asserted interest in keeping noncommercial stations free from controversial or partisan opinions not served by ban on station editorials, if such opinions could be aired through other programming).

Far from advancing the government's interest directly, the Statute "provides only the most limited incremental support for the interest asserted." *Bolger v. Youngs Drug Prods. Corp.*, 463 U.S. 60, 73 (1983). First, an intentional user of child pornography who is seeking a particular web site could circumvent a blocking order simply by using a different ISP that had not blocked that site. Second, as explained above, intentional users of child pornography frequently rely on "anonymizing" proxies to hide their on-line identity in an attempt to avoid prosecution. Such on-line anonymizers circumvent the null routing and DNS spoiling methods employed by ISPs to comply with the Informal Notices and blocking orders (as well as the "URL filtering" approach now advocated by the Defendant's expert). Thus, as a factual matter the existing Informal Notices pose virtually no barrier to pedophiles, nor would any future statutory blocking orders.

Third, as Plaintiffs' expert Michael Clark demonstrated in his Fourth Testimony (Supplemental TRO Exh. 16, filed under seal), the vast majority of all web sites blocked by IP address by AOL or Comcast either do not exist at all today or have moved IP addresses. Thus, in a substantial number of cases, the existing Informal Notices and blocking orders currently provide *no* beneficial effect whatsoever – but nevertheless obstruct access to protected expression.

All of this boils down to a simple conclusion: the widespread Internet censorship spawned by the Statute far outweighs any marginal advancement of the government's interest. *See Elrod v. Burns*, 427 U.S. 347, 361, 363 (1976). Given the more than one million web sites that have been blocked and the negligible effect of the Statute on the problem of child pornography, the Attorney General cannot meet his "burden of showing that the remedy [he] has adopted does not 'burden substantially more speech than is necessary to further the government's legitimate interests.'" *Turner*, 512 U.S. at 665 (quoting *Ward v. Rock Against Racism*, 491 U.S. 781, 799 (1989)). "[A] restriction of this scope is more extensive than the Constitution permits," *Bolger*, 463 U.S. at 73, and the Statute must be enjoined.

4. The Statute Is Not the Least Restrictive Means to Further the Governmental Interest.

In contrast to the ineffective Statute and its uniquely widespread impact on protected speech, other methods for fighting child pornography are both less restrictive and more effective. "When a plausible, less restrictive alternative is offered to a content-based speech restriction, it is the Government's obligation to prove that the alternative will be ineffective to achieve its goals." *Playboy Entertainment*, 529 U.S. at 816. That the Defendant cannot do.

First, the state may, and should, "vigorously enforce" existing laws, which already ban

child pornography. *Riley v. National Fed'n of the Blind of N.C., Inc.*, 487 U.S. 781, 800 (1988); *accord FCC v. League of Women Voters*, 468 U.S. at 398 (law is not narrowly tailored if government's goal is already served by "other regulatory means that intrude far less drastically upon [First Amendment] rights"); *Village of Schaumburg v. Citizens for a Better Env't*, 444 U.S. 620, 637 & n.11 (1980) (enforcement of existing laws against fraud would sufficiently serve purported governmental objective, therefore new law is not narrowly tailored). Under current law, the Attorney General can prosecute those responsible for the alleged child pornography, and work with local, federal and foreign authorities to go after child pornography at its source – its producers and distributors. Relying on such traditional criminal procedures results in no First Amendment harms – and has a far greater impact against the serious problem of child pornography than the Statute.[20]

Second, instead of expending efforts intimidating intermediary ISPs, the Attorney General could take the more effective and less burdensome approach of directly contacting the entity (usually a web hosting company or ISP) that is hosting the offending web site. Those entities have the ability to remove illegal sites from the Internet entirely, instead of leaving the sites blocked for some but not all of the Internet's users, as now happens under the Statute. *See* Deposition of John J. Burfete, Oct. 30, 2003, at 128-129 (hereafter "Burfete Dep."). When sites are blocked by a non-hosting ISP they are removed from the view of only that ISP's customers who do not use anonymizing proxies, but remain accessible to subscribers of other ISPs. That is, the actual offending material is still available – only one gateway to the material is partially

[20] Although pursuing and prosecuting child pornography creators and publishers overseas is obviously more challenging than a local prosecution, such efforts can be very successful. *See, e.g.,* U.S. Customs Service Press Release, "U.S. Customs Service, Russian Policy Take Down Global Child Pornography Web Site," March 26, 2001, *available at* http://www.cbp.gov/hot-news/pressrel/2001/0326-00.htm; U.S. Customs Today, "U.S. Customs, Moscow City Police team up against child pornography," April 2001, *available at* http://www.cbp.gov/xp/CustomsToday/2001/April/custoday_bluorchid.xml.

blocked. In contrast, when a web host takes down offending material, it is completely removed from the Internet and no longer available to anyone. AOL's representative testified to his belief that removing the content at the web hosting company level "would be a better resolution because . . . the content would be removed from the Internet" and not just for AOL customers. AOL Dep. at 74-75.

Furthermore, according to Defendant's own expert, web hosting companies and ISPs usually respond with alacrity to complaints involving child pornography. *See* Stern Report at 6.[21] According to an employee of the Attorney General's Office, web hosting companies are known to be universal in their opposition to child pornography. Burfete Dep. at 106-107. Indeed, a Verizon representative stated that he had never experienced a hosting company's refusal to take down child pornography – "[b]ased on five years of working closely with law enforcement in the . . . Internet community, I've never come across a non-cooperative entity when it came to child pornography." Verizon/Lebredo Dep. at 91. When Verizon receives a child pornography complaint, it initiates an established process for finding the owner of the relevant web hosting service through an online database, using that information to contact the host directly either via email or telephone, and explaining that Verizon had received a complaint that child pornography was being hosted on its servers. Verizon then provides the web host with the web address so that it can respond. According to Verizon, "in most instances the reaction [is] quite expeditious." Verizon/Lebredo Dep. at 93.

Likewise, WorldCom explained in its deposition that the task of contacting the web hosting company is easy to undertake and appears to be effective most (if not all) of the time. WorldCom Dep. at 78-89. WorldCom used this method itself in an attempt to address an

[21] Some web hosts make it very easy for Internet users to report child pornography; for example, terra.es even offers an email address specifically for reporting child pornography. WorldCom Dep. at 83.

Informal Notice it received without blocking innocent Internet content. When the Attorney General sent WorldCom its first Informal Notice, the company first determined the identity of the hosting ISP, a process that took less than five minutes. WorldCom Dep. at 79-80. WorldCom notified by email and phone that hosting ISP that it might have child pornography on its servers and received an overnight response. *Id*. at 82-83. Within two days WorldCom determined that that particular web site had been removed entirely from the Internet. *Id*. at 87-88. With a few simple phone calls, WorldCom was able to achieve a result – the removal of a particular piece of child pornography from the Internet entirely – that the Attorney General has not accomplished in nearly two years of issuing hundreds of Informal Notices.

In recognition of the effectiveness of contacting the hosting ISP, the Attorney General's office also has used this method in a limited number of cases. Burfete Dep. at 121-123. The office even prepared statements of recommended language for telephone contact with Web Hosting Services requesting that they remove posted child pornography. *See* Supplemental TRO Exh. 18. When investigators were given information about a web hosting service that is hosting child pornography, they would contact the host and ask them to remove the offending materials from their service. *See* Supplemental TRO Exhs. 15, 16, 18; Burfete Dep. at 121-123.

Both criminal prosecutions and the process of contacting web hosts to take down child pornography from the Internet are plainly more effective than the Statute in combating this serious problem, yet they intrude far less on constitutionally protected speech. The Defendant cannot meet his burden of proving otherwise. Far from being the least restrictive alternative, the Statute is one of the most speech-restrictive options that the state could have devised, yet with little benefit in the fight against child pornography. Simply put, government may not "burn the house to roast the pig." *Butler v. Michigan*, 352 U.S. 380, 383 (1957). Here, the government has

burned thousands of entire farms in thousands of villages across the countryside, while several hundred targeted pigs are barely singed.

The importance of this case cannot be overstated. As discussed more below, this case raises grave First Amendment implications for the viability of the Internet as a "vast democratic for[um]," where anyone can be a publisher and vast libraries of information are available at the touch of a button. *Reno v. ACLU*, 521 U.S. at 853, 868. In this case, the Attorney General in one state directed ISP blocking orders at just a few hundred illegal web sites – and as a result more than a thousand times more legal sites were blocked. Statistically, for each illegal web site targeted, more than one thousand lawful sites were blocked. If this law were duplicated in fifty states and vigorously enforced by even a few state officials, the Internet – a precious resource that has become a vital medium for exercising First Amendment rights – would be severely compromised. The Pennsylvania Statute sets a dangerous precedent, and it is critical to the future of the Internet that it be struck down.

B. The Statute Lacks the Procedural Safeguards Necessary to Overcome the Heavy Presumption Against Prior Restraints.

The Statute also must be enjoined because of its striking procedural deficiencies. It plainly violates the requirement that any prior restraint of speech "'take[ ] place under procedural safeguards designed to obviate the dangers of a censorship system.'" *Southeastern Promotions, Ltd. v. Conrad*, 420 U.S. 546, 560 (1975) (quoting *Freedman v. Maryland*, 380 U.S. 51, 58 (1965)). Indeed, there is a "*heavy presumption* against [the] constitutional validity" of any prior restraint of speech. *Bantam Books, Inc. v. Sullivan,* 372 U.S. 58, 70 (1963) (emphasis added); *see also Freedman*, 380 U.S. at 459 ("The presumption against prior restraints is heavier – and the degree of protection broader – than that against limits on expression imposed by criminal

penalties."); *Southeastern Promotions*, 420 U.S. at 558-59; *Organization for a Better Austin*, 402 U.S. at 419; *Gascoe, Ltd. v. Newtown Township*, 699 F. Supp. 1092, 1098 (E.D. Pa. 1988).

Under the Statute, the state Attorney General or any county district attorney can apply to a local judge for an order declaring that (a) certain web site content on the Internet is probably child pornography, and (b) the web site can be accessed through the services of a particular ISP(s). The application proceeding can go forward on an *ex parte* basis, without the participation of (or even prior notice to) the ISP or the web site owner, and no post-hearing notice to the web site owner. *See* 18 Pa. Stat. Ann. § 7627. If the court makes this *ex parte* probable cause determination, the state Attorney General notifies the ISP in question, and the ISP then has five days in which to block all access to the specified web site, or else face criminal liability. *See id.* §§ 7624, 7627-28.

These woefully inadequate procedures fly in the face of more than forty years of Supreme Court precedent. The Court has declared its "insistence that regulations of obscenity scrupulously embody the most rigorous procedural safeguards," *Bantam Books*, 372 U.S. at 66, yet the Pennsylvania Statute has virtually none. The Statute does not even provide for the most basic procedure of all: an adversary hearing, prior to the web site being blocked. Furthermore, the statute directs the judge to determine only whether there is "probable cause" that the content of the websites is illegal speech – a standard that the Supreme Court has rejected outright as constitutionally inadequate.

1. The Lack of Any Adversarial Hearing is Alone Fatal.

The Statute totally fails to provide the constitutionally required procedures necessary before any restraint can be imposed on speech – including allegedly illegal speech like obscenity or child pornography, *see Marcus v. Search Warrants of Prop. at 104 E. 10th St.*, 367 U.S 717,

731 (1961) ("a State is not free to adopt whatever procedures it pleases for dealing with obscenity . . . without regard to the possible consequences for constitutionally protected speech"). In a long line of cases, the Supreme Court has articulated clear procedures that must be followed, including (a) an adversarial hearing, (b) with the burden on the censor, and (c) with clear opportunity for prompt judicial review and appeal. *See, e.g., Freedman*, 380 U.S. at 58-59; *Southeastern Promotions*, 420 U.S. at 560; *FW/PBS, Inc. v. City of Dallas*, 493 U.S. 215, 227 (1990). Because the Pennsylvania Statute does not provide for an adversarial hearing – the most fundamental of procedures, and the procedure on which each of the other requirements is based – it violates the First Amendment.

The Supreme Court has plainly and repeatedly made clear that as a threshold matter, an adversarial hearing *must* take place whenever speech is to be restrained. In *Freedman v. Maryland*, the Court held that:

> because only *a judicial determination in an adversary proceeding* ensures the necessary sensitivity to freedom of expression, only a procedure requiring a judicial determination suffices to impose a valid final restraint.

380 U.S. at 58 (emphasis added); *see also Southeastern Promotions*, 420 U.S. at 560 (same); *Heller v. New York*, 413 U.S. 483, 489 (1973) ; *United States v. Thirty-seven Photographs*, 402 U.S. 363, 367 (1971); *Kingsley Books, Inc. v. Brown*, 354 U.S. 436, 440 (1957) ("the issue of obscenity must be promptly tried and adjudicated in an adversary proceeding for which adequate notice, judicial hearing, and fair determination are assured"). Here, although the Statute requires judicial approval of an application, it does not require an adversarial proceeding. In similar circumstances in *Marcus v. Search Warrants*, the Supreme Court rejected a statutory scheme that permitted seizure of allegedly obscene materials prior to an adversary hearing, even though a judge approved the seizure in an *ex parte* proceeding. 367 U.S at 731, 735.

Worse yet, not only are the ISP and the web site owner not participants in the application process, they are not even notified that it is occurring. The first that an ISP will learn of it is upon receiving the court order demanding that it block access to certain web sites within five days. And the web site owner whose speech is directly curtailed is never notified by the Attorney General or the court, nor are the owners of innocent sites that have been blocked as a result. The lack of an adversarial hearing, in and of itself, is fatal to the Statute.[22]

2. The Lack of a Prior Hearing is Also Fatal.

The Statute has yet another fatal procedural error: It fails to require an adversarial hearing *before* the ISP must block access to the web site in question. The Supreme Court has held that a "publication may not be taken out of circulation completely until there has been a determination of [illegality] after an adversary hearing." *Fort Wayne Books, Inc. v. Indiana*, 489 U.S. 46, 63 (1989); s*ee also Heller*, 413 U.S. at 492-93; *Marcus*, 367 U.S. at 735; *ACLU v. City of Pittsburgh*, 586 F. Supp. 417, 423-24 (W.D. Pa. 1984). The Statute does just that – it denies access to certain web site content, thereby essentially removing it from "circulation," without a prior hearing, in violation of the First Amendment.

The question of whether the adversarial hearing must take place before the restraint occurs has been most squarely considered in the context of seizures of expressive material. What is relevant in the seizure cases is whether the seizure has the effect of precluding all access to a challenged piece of expressive material. Thus, a single copy of a challenged work can be seized without prior hearing in order to preserve evidence for a criminal proceeding, on the theory that the public can still view other copies of the work during adjudication. *See Heller*, 413 U.S. at

[22] Of course, the *Freedman* requirement that the censor must bear the burden of proof in court cannot be satisfied in a non-adversarial process. Likewise, *Freedman* makes clear that the requirement of prompt judicial review and appeal can only be satisfied if that process is adversarial.

492 & n.8. But when the goal or effect of the seizure is to block the public's access to a challenged work, the adversarial hearing must take place *before* the seizure. *See Fort Wayne Books*, 489 U.S. at 63.

Although the Pennsylvania Statute does not authorize a physical "seizure," the effect is identical – essentially, the Statute "seizes" (or at least outlaws) the method of distribution of the challenged web sites. Because the goal and effect of the governmental action is to foreclose the public's access to challenged material, there must be a hearing prior to that "seizure" going into effect. *See Fort Wayne Books*, 489 U.S. at 63-65, 67 (overturning a seizure because the adversarial hearing took place *after* the seizure). The Statute provides for no adversarial hearing whatsoever. Because of this defect, no proceeding under the Statute can be constitutional, and the Statute must be enjoined.

3. The Reliance on "Probable Cause" is Unconstitutional.

The Statute has a third procedural defect, which also renders it unconstitutional. Under the Statute, an order can be entered against a web site based solely on a judicial determination that the challenged content "constitute[s] probable cause evidence of a violation of section 6312 [the child pornography statute]." 18 Pa. Stat. Ann. § 7627. This reliance on a "probable cause" standard is directly contrary to a long line of Supreme Court cases that hold that probable cause is not enough to support the suppression of expression. Rather, a court must make a final determination, under applicable standards, whether the materials at issue are protected by the First Amendment.

The Supreme Court has specifically recognized that among "the special rules applicable to removing First Amendment materials from circulation" is "the admonition that probable cause to believe that there are valid grounds for seizure is insufficient to interrupt the sale of

presumptively protected books and films." *Fort Wayne Books*, 489 U.S. 65-66. The Court has noted that its cases "firmly hold that mere probable cause to believe a legal violation has transpired is not adequate to remove books or films from circulation." *Id. See also, e.g., New York v. P.J. Video, Inc.*, 475 U.S. 868 (1986); *Blount v. Rizzi*, 400 U.S 410, 420 (1971) (a court cannot prohibit the distribution of materials via U.S mail based solely on a probable cause determination of obscenity). A court cannot deny access to First Amendment materials because it determines they are probably illegal; it must determine that they *are* illegal.

Here, the Pennsylvania Attorney General has alleged that certain web sites contain child pornography. The First Amendment requires that before blocking access to those sites, a court must apply the standards in *New York v. Ferber*, 458 U.S. 747 (1982), and *Ashcroft v. Free Speech Coalition*, 535 U.S 234 (2002), which address the constitutional limits of child pornography laws, and come to a definitive conclusion about whether the web sites contain illegal materials. In contrast, the Statute expressly and exclusively directs the court to determine whether there is mere "probable cause" that the materials are illegal. Because of this defect, no proceeding under the Statute can be constitutional, and the Statute must be enjoined.

C. The Fact That the Statute is Aimed at Child Pornography Does Not Change The Applicable Legal Analysis.

These procedural requirements are not altered by the fact that the Statute is aimed at child pornography. In discussions with the parties during this litigation, the Court posed the question of whether the analysis found in *United States v. Moore*, 215 F.3d 681 (7th Cir.), *cert. denied*, 531 U.S. 915 (2000), should affect the Court's consideration of the issues raised in this case. *Moore* does not support the application of any yet-to-be-defined lower procedural standard to this case.

As an initial matter, the *Moore* decision itself made expressly clear that its decision focused on an arrest warrant for an individual, and thus did not involve a prior restraint on any speech (lawful or not). The court wrote:

> The arrest of a suspect for possession of contraband does not constitute a prior restraint in the way the seizure of books or films does. While at first glance it may seem odd to require more judicial protection for the liberty of one's books than for one's body, the distinction reflects this country's great concern with the chilling effect on protected speech brought on by a government seizure. An ordinary arrest implicates an individual's Fourth Amendment freedoms and must meet the constitutional standard of reasonableness. The seizure of an individual's books implicates both First and Fourth Amendment liberties, for which the Supreme Court has required heightened judicial protection to afford the right to free expression the breathing room it needs to survive. In some circumstances, an arrest might implicate First Amendment rights as well, but Moore's arrest did not act as a prior restraint, and therefore we need not reach that issue.

Id. at 685. The court in *Moore* thus made clear that its primary analysis would have been different if a prior restraint were present (as is present in the case before this Court).

More fundamentally, the *Moore* court's contrasting of obscenity standards with child pornography standards was very specifically focused on the narrow question before the court in that case – whether a pre-arrest judicial determination that certain material was child pornography was required. The *Moore* court's analysis is applicable only to that narrow question. The court reasoned that the substantive standard of proof in obscenity cases (under *Miller v. California*, 413 U.S. 15, 24-25 (1973)) was significantly more complex than that required in child pornography cases (under *Ferber*, 458 U.S. at 764-65). The *Moore* court then decided that:

> The application of child pornography standards involves a more limited inquiry than *Miller* requires, *see Ferber*, 458 U.S. at 764-65, and is within the competency and experience of police officers making a probable cause determination.

Id. at 686. Thus, to the extent the *Moore* decision can be read to support some lesser procedure in child pornography cases, the language of that decision is solely and exclusively focused on the question of a pre-arrest warrant, where the ability of a police officer to make a reasoned and timely judgment is critical. No language in *Moore* suggests that the Seventh Circuit was making any broader pronouncement.

Furthermore, the Supreme Court's two major cases on child pornography and the First Amendment make clear that the same procedural requirements apply as in obscenity cases. The very starting point of the Supreme Court's seminal child pornography decision in *Ferber* was a recognition that child pornography laws can infringe on protected speech just as much as obscenity laws:

> Like obscenity statutes, laws directed at the dissemination of child pornography run the risk of suppressing protected expression by allowing the hand of the censor to become unduly heavy.

Ferber, 458 U.S. at 756. The *Ferber* decision did conclude that the seriousness of child pornography warranted a different substantive standard than for obscenity, such that some non-obscene pictures of children would nonetheless be unprotected. But nothing in the *Ferber* decision suggests that the *procedural* safeguards of the First Amendment should also be lowered.

In other words, the *Ferber* court recognized and accounted for the different governmental interest in obscenity and child pornography by lowering the substantive standards. The *Ferber* Court did not do anything to alter the First Amendment procedures that apply to prior restraints (whether arising out of an obscenity or child pornography law). Indeed, the *Ferber* Court made explicitly clear that the First Amendment still required a searching analysis of any restraint on speech, and that there might be some circumstances in which even content involving sexual conduct by minors would be constitutionally protected expression. *See Ferber*, 458 U.S. at 773-

74 (discussing material with serious value); *see also Free Speech Coalition*, 535 U.S at 247-51. The Court then instructed that such situations "should be cured through case-by-case analysis of the fact situations to which [a law's] sections . . . may not be applied." *Id.* at 774. Implicit in the Court's reliance on this "case-by-case analysis" is the assumption that the normal procedures under the First Amendment would allow an opportunity for such an analysis. Any contrary conclusion – that the First Amendment procedures could be discarded in child pornography cases – would directly lead to the risk identified in *Ferber*: that under a child pornography law "the hand of the censor [would] become unduly heavy." *Id.* at 756. In the case now before this Court, the blocking of more than one million innocent web sites surely constitutes an "unduly heavy" hand.

The Supreme Court's 2002 decision in *Free Speech Coalition* further supports the need for strict procedural requirements in child pornography cases, including a hearing prior to the restraint of speech. In that case, the Supreme Court struck down a federal child pornography statute precisely because of its impact on *protected* expression. The Supreme Court could not have been more clear:

> The Government may not suppress lawful speech as the means to suppress unlawful speech. . . . "[T]he possible harm to society in permitting some unprotected speech to go unpunished is outweighed by the possibility that protected speech of others may be muted. . . ."

Id. at 255 (quoting *Broadrick*, 413 U.S at 612). It is precisely the risk to protected expression, which looms so large in this case, that necessitates a hearing before restraining speech. Furthermore, *Free Speech Coalition* (decided two years after *Moore*) calls into question the very factual premise that *Moore* relied on. In that case the Supreme Court explained that given current technology it might not always be that easy to discern the difference between web sites that depict real children (and are therefore *per se* unprotected) and those that contain only

computer-generated images (and are therefore protected unless they are obscene, which *Moore* has acknowledged is a complex inquiry). 535 U.S. at 241.

But even accepting *Moore*'s premise that child pornography is easier for a police officer to detect than obscenity, that does not justify the widespread removal from circulation without a prior hearing at issue here. This case is fundamentally different from one where the police are seizing hard-copy materials such as magazines or videos that they believe are child pornography, where there can be no question that little or no additional protected speech is affected by the seizure. Here the Defendant *knew* that because of the technological reality of the Internet, the removal of some web sites that he believed contained child pornography would also result in protected web sites being blocked. *See* WorldCom Dep. at 17-22, 60-61, 115-117; AOL Dep. at 43-47. The risk that there would be such a widespread effect on protected expression renders a prior hearing absolutely essential.[23]

As both *Ferber* and *Free Speech Coalition* make clear, the fact that a law is labeled as one attacking child pornography cannot insulate it from traditional First Amendment review. What is relevant is not the law's label, but its impact on protected expression, which in the case now before this Court is immense.

D. The Statute Provides No Notice or Opportunity to be Heard to ISPs, Speakers or Listeners, and Thus Violates Principles of Procedural Due Process Under the Fourteenth Amendment.

In addition to flouting First Amendment procedural constraints, the Pennsylvania Statute also violates closely related Fourteenth Amendment procedural due process rights.

[23] Even were *Moore*'s analysis credible in suggesting some loosening of pre-seizure procedural constraints in cases of alleged child pornography, it would provide no basis for the scheme before this court. Neither the Statute nor the Informal Notices provide for any adversary hearing whatsoever – whether before or after seizure – on the actual (as opposed to the probable) status of the allegedly offending websites.

When the government seeks to deprive an individual of a liberty interest protected by the Fourteenth Amendment – such as the First Amendment right to free speech – the government must follow certain procedural requirements. *See, e.g., United States v. Raffoul*, 826 F.2d 218, 222 (3d Cir. 1987). At a minimum, individuals have the right to "notice and an opportunity for a hearing appropriate to the nature of the case." *Id.* (citing *Goss v. Lopez*, 419 U.S. 565 (1975)). Notice is required to inform individuals of a hearing that might affect their rights, and allow them time for adequate preparation. *See Memphis Light, Gas and Water Div. v. Craft*, 436 U.S. 1, 13 (1978) (describing notice as an "'elementary and fundamental requirement of due process . . . to apprise interested parties of the pendency of the action and afford them an opportunity to present their objections'") (quoting *Mullane v. Central Hanover Bank & Trust Co.*, 339 U.S 306, 313 (1950)). And, of course, "[t]he right to be heard before being condemned to suffer grievous loss of any kind . . . is a principle basic to our society." *Mathews v. Eldridge*, 424 U.S. 319, 333 (1976) (internal quotation marks and citation omitted).

The Pennsylvania Statute meets neither of these minimum requirements with respect to web site owners, Internet users or ISPs. First, owners of web sites that have been identified by the Attorney General as containing child pornography are never notified that proceedings challenging the legality of their sites are occurring or have occurred, even if the court has issued orders requiring that access to those sites be blocked. Those web site owners also have no opportunity to participate in those hearings and defend their sites. Worse yet, potentially millions of web sites that the Pennsylvania Attorney General has *not* identified as child pornography have been blocked as a result of the Informal Notice process, and would also have been blocked had he used the Statutory process. The owners of those entirely legal web sites also have not received – and under the Statute, would not receive – any notice that their sites

have been blocked or any hearing to challenge the blocking orders. This is censorship at its worst. The only way that a web site owner might discover that access to its site has been blocked is if it happens to notice that web site traffic has decreased substantially and investigates.[24] With respect to web site owners, including both those targeted by the blocking orders and the innocent by-standers whose sites also have been or would be blocked, the Statute creates a clear Fourteenth Amendment violation by not providing for notice and an opportunity to be heard.

Second, the Statute denies Internet users their First Amendment right to receive information, also without the process that is due under the Fourteenth Amendment. "Freedom of speech presupposes a willing speaker. But where a speaker exists, . . . the protection afforded is to the communication, to its source and to its recipients both." *Virginia State Bd. of Pharmacy*, 425 U.S. at 756-57; *see also* Section I, *supra*. Just as with the web site owners (the speakers), Internet users (the recipients) are never notified that they have been denied access to certain web sites, including potentially more than a million entirely legal sites, and they have no ability to participate in any hearing on that issue.

Finally, the Statute also violates the Due Process Clause as it applies to ISPs. The Statute permits the court to make its probable cause determination on an *ex parte* basis, meaning that an ISP receives no notice before the hearing occurs. Rather, the ISP is notified only after the fact that a particular web site has been deemed probably illegal, and then has five days to ensure that access to that site is blocked before it faces criminal penalties. As to the opportunity to be heard, the Statute provides ISPs with no right to participate in a hearing before or after the order is issued. ISPs' fundamental right "to be heard at a meaningful time and in a meaningful manner,"

[24] For example, AOL testified in its deposition to an incident in which a single Informal Notice led to the blocking of access to more than 400,000 unrelated web sites. In that situation, the web hosting company that hosted the blocked sites noticed a dramatic drop in traffic to hundreds of thousand of web sites. It took the hosting company days to investigate, contact AOL, and get AOL to unblock the sites. AOL Dep. at 54-62.

Mathews, 424 U.S. at 333 (internal quotation marks and citation omitted), has plainly been violated, and the Statute must be enjoined.

IV. THE INFORMAL NOTICES VIOLATE BOTH THE FIRST AND FOURTEENTH AMENDMENTS.

Most of the Attorney General's actions in implementing the Statute have been taken pursuant to his Informal Notice scheme, rather than the procedures set forth in the Statute. Indeed, it is the compliance with a few hundred Informal Notices that has actually resulted in more than one million innocent web sites being blocked. The Informal Notice scheme has the same constitutional defects that the Statutes does, but with even fewer procedures. Accordingly, it presents an even clearer constitutional violation. This Court should enjoin any future use of Informal Notices, and declare that those already issued are legally ineffective.

A. The System of Informal Notices is Plainly Unconstitutional and Must Be Permanently Enjoined.

1. The System is Squarely Contrary to *Bantam Books*.

As Plaintiffs demonstrated in their initial request for a temporary restraining order in September, the secret "Informal Notice" censorship system of the Attorney General is remarkably similar to the government scheme struck down in the landmark 1963 Supreme Court decision in *Bantam Books, Inc. v. Sullivan,* 372 U.S. 58 (1963); indeed, the primary difference is that the Attorney General's scheme is more egregious than that in *Bantam Books* because it was done in secret. Accordingly, this Court should make permanent its temporary order of September 9, 2003, that the Attorney General "discontinue issuance of informal notices to internet service providers requiring that they deny their subscribers access to any website." Order, *CDT v. Fisher,* No. 03-5051 (E.D. Pa. Sept. 9, 2003).

In *Bantam Books,* a Rhode Island state commission used "informal" notices to advise

book distributors that certain books and materials were deemed "objectionable" by the commission. The commission asked for the distributors' "cooperation" in removing the material from their news stands, without opportunity for judicial review, and advised them of the commission's duty to recommend prosecution. The Supreme Court held that this form of informal censorship violated the First and Fourteenth Amendments because "it provide[d] no safeguards whatever against the suppression of nonobscene, and therefore constitutionally protected, matter." *Bantam Books,* 372 U.S. at 71. That the government censorship came in the form of an "informal" notification did not affect the First Amendment analysis because courts must "look through forms to the substance" of government conduct, and there the government was taking coercive action. *Id*. at 67.

The Pennsylvania Attorney General censorship system is directly parallel to the "informal" system struck down forty years ago in *Bantam Books*. The Attorney General alone has decided what web sites should be taken down and notified the ISPs (the "distributors" in the Internet context) to remove them, without any prior notice or opportunity for judicial review. The Attorney General calls his system an "informal" one, but his notices implicitly threatened further action if the offending web site was not taken down within five days and if the ISP did not provide proof that it has been taken down. The Attorney General was not "advising the [ISPs] of their legal rights and liabilities," *Bantam Books*, 372 U.S. at 72, which is the type of informal contact that would be permissible; rather, he was *ordering* them to block Internet content[25] – and they complied, which further demonstrates the coercive nature of those notices. *See, e.g., Neiderhiser v. Berwick*, 840 F.2d 213, 216-17 (3d Cir. 1988) (city's attempt to indirectly compel compliance with statute banning sale of lewd materials was basis for First and

[25] For more about the Attorney General's coercive actions, *see* Section IV.B, *infra*.

Fourteenth Amendment claims); *White v. Lee*, 227 F.3d 1214, 1228 (9th Cir. 2000) ("This court has held that government officials violate [the First Amendment] when their acts 'would chill or silence a person of ordinary firmness from future First Amendment activities.'") (quoting *Mendocino Envtl. Ctr. v. Mendocino County*, 192 F.3d 1283, 1300 (9th Cir. 1999)); *Rattner v. Netburn*, 930 F.2d 204, 208-210 (2d Cir. 1991) ("'where comments of a government official can reasonably be interpreted as intimating that some form of punishment or adverse regulatory action will follow the failure to accede to the official's request, a valid claim for violation of First Amendment rights can be stated'") (quoting *Hammerhead Enters., Inc. v. Brezenoff*, 707 F.2d 33, 39 (2d Cir. 1983)); *ACLU v. Pittsburgh*, 586 F. Supp. at 421-23 (finding that mayor's informal intimidation of retailers to remove magazines from their shelves constituted a prior restraint that sufficiently suppressed speech). Thus, just as in *Bantam Books*, the Attorney General's form of "informal censorship . . . sufficiently inhibit[s] the circulation of publications to warrant injunctive relief." *Bantam Books*, 372 U.S. at 67 (citations omitted).

2. The System's Utter Lack of Procedures Violates the First and Fourteenth Amendments.

The direct parallel to *Bantam Books* is all that is needed to permanently enjoin the use of Informal Notices. But the Informal Notice scheme fails for yet another reason: It lacks any protective procedures, and therefore violates the First and Fourteenth Amendments.

The Informal Notice system violates the First Amendment because it does not include even the minimum procedures necessary to protect important free speech rights, such as an adversarial process, prompt judicial review, and use of the proper standard for assessing the legality of speech. *See* Sections III.B.1 & III.B.2, *supra*. Like the Statute, the Informal Notice system permits no adversarial hearing whatsoever before *or* after the governmental action to block access to the challenged web sites. Worse yet, it directly violates *Freedman v. Maryland*'s edict

that there be a prompt judicial determination with the burden on the government to prove the illegality of the speech at issue. 380 U.S. at 58-59. Not only does the Attorney General's informal notice scheme provide no opportunity for judicial review, but also it includes no procedure whatsoever for determining whether the affected web site constitutes unprotected speech – it is left to the sole discretion of the Defendant. Indeed, neither the web site owner nor the public is ever informed that the Attorney General has required that a web site be blocked, making it virtually impossible to challenge his decision. This not only impermissibly places the burden of proving legality on the speaker, it prevents the speaker from knowing that such a burden has been placed on it in the first place.

The Informal Notice system also violates the Fourteenth Amendment by not meeting the minimum procedural due process requirements of notice and an opportunity to be heard. *See* Section III.D, *supra*. No affected parties – not the ISPs, not the targeted web site owners, not the owners of innocent blocked sites, not Internet users – are afforded any hearing under the Informal Notice system, and only the ISP was notified that a particular web site was to be blocked. This does not satisfy the dictates of the Fourteenth Amendment.

3. The System Violates the Substantive Requirements of the First Amendment.

Finally, as already made clear in Section III.A., *infra*, the Informal Notice scheme plainly violates the First Amendment because of its effects on protected speech. Just like the Statute, the Informal Notice scheme is unconstitutionally overbroad, and cannot satisfy strict scrutiny because it is neither effective at combating child pornography nor the least restrictive means for doing so.

B. The Outstanding Informal Notices Must Be Declared Null and Void.

Given that the Informal Notice system is unconstitutional and its future use must be enjoined, it follows that the Informal Notices already issued pursuant to that system are invalid. Accordingly, Plaintiffs also ask this Court to issue: (1) a declaration that the existing Informal Notices have no legal effect; (2) a prospective injunction ordering the Defendant to take no action against any recipients of Informal Notices arising from their failure to comply with those Informal Notices; and (3) an order that the Defendant deliver a copy of that injunction to all recipients of an Informal Notice.

Such relief from compliance with the existing Informal Notices is crucial, given that those Informal Notices are today responsible for the blocking of a truly massive amount of content – more than 600,000 web sites.[26] Indeed, the impact on wholly lawful speech is unprecedented in its scope. More than 600,000 web site owners – about the population of Washington, DC – are being denied their right to speak, and millions of Internet users are being denied their right to listen. The current situation is absolutely untenable from a First Amendment perspective, given that any "loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury." *Elrod*, 427 U.S. at 373. It is time to remedy this needless loss of speech.

Indeed, the only reason that this lawsuit and Plaintiffs' motions were not brought sooner is that the Attorney General operated his censorship scheme in utter secrecy, without informing either the public or any of the hundreds of thousands of innocent web sites blocked as a result of the Informal Notices – even though he knew the blocking of innocent sites was the inevitable

[26] Plaintiffs could have sought in September to overturn the existing Informal Notices. Plaintiffs chose instead to defer that request until Plaintiffs were able to demonstrate the harmful impact of the entire scheme.

result of the Informal Notices. *See* WorldCom Dep. at 17-22, 60-61,115-117 (explaining that various ISPs had warned the Attorney General's Office repeatedly about the problems with implementing the Statute); AOL Dep. at 43-47 (same). When Plaintiff CDT found out that the Attorney General was issuing Informal Notices and attempted to obtain information from him to evaluate whether innocent sites had been blocked, he stonewalled for months, leading Plaintiffs to conclude that litigation was their only option. It has only been in the past month, as a result of discovery in this lawsuit, that Plaintiffs have discovered the shocking magnitude of the amount of blocked speech.

Furthermore, it is important to declare the invalidity of the Informal Notices because those orders are not mere voluntary requests for compliance that the ISPs can choose to ignore. Rather, they are coercive edicts from the state's chief prosecutor, and contain implicit threats of prosecution. *See* TRO Exh. 1. In fact, AOL was explicitly "told by [the Attorney General's Office] that the informal notice from the Attorney General had the same force and effect as a court order and that [ISPs] were obliged to comply with it as if it were a court order." AOL Dep. at 101. Needless to say, the ISPs who received them did view them as orders with which they must comply, and believed they faced serious legal (or publicity) risks if they did not. *See, e.g.,* AOL Dep. at 100-103; WorldCom Dep. at 114-117.

The Attorney General also engaged in aggressive public intimidation of those who challenged his secret censorship scheme. For example, after WorldCom wrote to the Attorney General's Office to suggest that it should use the statutory procedures instead of the secret Informal Notices, the Attorney General issued a press release accusing WorldCom of refusing to block child pornography. *See* TRO Exh. 2; WorldCom Dep. at 113-14. Since the issuance of that press release, no ISP has refused to follow any of the secret Informal Notices.

In sum, to adequately remedy the far-reaching infringement of First Amendment rights in this case, this Court must declare the Informal Notices invalid, enjoin the Attorney General from taking any action against an ISP for failing to comply with an Informal Notice, and require the Attorney General to notify the ISPs of the court's order.

V. BOTH THE STATUTE AND THE INFORMAL NOTICES VIOLATE THE COMMERCE CLAUSE OF THE UNITED STATES CONSTITUTION.

Finally, both the Statute and the Informal Notices violate the Commerce Clause of the United States Constitution (U.S. Const., Art. I, § 8, cl.3). Because of the global nature of the Internet and the fact that most ISP's networks cross state boundaries, the blocking orders[27] challenged in this litigation impose restrictions on communications occurring wholly outside of Pennsylvania, effect an impermissible burden on interstate commerce, and risk subjecting Internet speech to inconsistent state obligations.

A. The Statute and Informal Notices Are *Per Se* Invalid Because They Regulate Commerce Entirely Outside the State of Pennsylvania.

A state statute that "has the 'practical effect' of regulating commerce occurring wholly outside that State's borders is invalid under the Commerce Clause." *Healy v. Beer Inst.*, 491 U.S. 324, 336 (1989).[28] *See also Edgar v. MITE Corp.*, 457 U.S. 624, 642-43 (1982) (the "Commerce Clause . . . precludes the application of a state statute to commerce that takes place wholly outside of the State's borders"); *Brown-Forman Distillers Corp. v. New York State*

[27] Some of the ISPs (such as Epix.com) that have received Informal Notices operate only within the state of Pennsylvania, and thus Notices to those ISPs may not interfere with speech between one non-Pennsylvania state and another. But a majority of the blocking orders would affect speech wholly outside of Pennsylvania. In any event, even blocking orders to intra-state ISPs such as Epix.com directly regulate interstate communications, and directly create a risk of inconsistent state regulations.

[28] The Supreme Court has long recognized that the Commerce Clause encompasses an implicit or "dormant" limitation on the authority of the states to enact legislation affecting interstate commerce. *See Healy*, 491 U.S. at 326 n.1; *Hughes v. Oklahoma*, 441 U.S. 322, 326 & n.2 (1979).

Liquor Auth., 476 U.S. 573, 582 (1986) (state liquor statute directly regulated out-of-state transactions in violation of the Commerce Clause).

The Commerce Clause limitation on state regulation has been squarely applied to communications over the Internet. In *American Library Association v. Pataki*, 969 F. Supp. 160 (S.D.N.Y. 1997), the district court struck down a New York statute whose impact on interstate speech was far less direct than the Statute and Informal Notices challenged here. In that case, the court wrote:

> The unique nature of the Internet highlights the likelihood that a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent regulation by states that the actor never intended to reach and possibly was unaware were being accessed. Typically, states' jurisdictional limits are related to geography; geography, however, is a virtually meaningless construct on the Internet. The menace of inconsistent state regulation invites analysis under the Commerce Clause of the Constitution, because that clause represented the framers' reaction to overreaching by the individual states that might jeopardize the growth of the nation – and in particular, the national infrastructure of communications and trade – as a whole. . . .
>
> The Commerce Clause is more than an affirmative grant of power to Congress. As long ago as 1824, Justice Johnson in his concurring opinion in *Gibbons v. Ogden*, 22 U.S. 1, 9 Wheat. 1, 231-32, 239, 6 L. Ed. 23 (1824), recognized that the Commerce Clause has a negative sweep as well. In what commentators have come to term its negative or "dormant" aspect, the Commerce Clause restricts the individual states' interference with the flow of interstate commerce in two ways. The Clause prohibits discrimination aimed directly at interstate commerce, . . . and bars state regulations that, although facially nondiscriminatory, unduly burden interstate commerce. . . . Moreover, courts have long held that state regulation of those aspects of commerce that by their unique nature demand cohesive national treatment is offensive to the Commerce Clause. *See, e.g.*, *Wabash, St. L. & P. Ry. Co. v. Illinois*, 118 U.S. 557 (1887) (holding railroad rates exempt from state regulation).
>
> . . . [The challenged New York law] contravenes the Commerce Clause for three reasons. First, the Act represents an unconstitutional projection of New York law into conduct that occurs wholly outside New York. Second, the Act is invalid because although [the governmental interest] is a legitimate and indisputably worthy subject of state legislation, the burdens

> on interstate commerce resulting from the Act clearly exceed any local benefit derived from it. Finally, the Internet is one of those areas of commerce that must be marked off as a national preserve to protect users from inconsistent legislation that, taken to its most extreme, could paralyze development of the Internet altogether. Thus, the Commerce Clause ordains that only Congress can legislate in this area, subject, of course, to whatever limitations other provisions of the Constitution (such as the First Amendment) may require.

Id. at 168-69.[29] Since *Pataki*, many courts have struck down on Commerce Clause grounds state laws that attempt to regulate the Internet. *See, e.g., American Booksellers Foundation v. Dean*, 342 F.3d 96 (2d Cir. 2003); *ACLU v. Johnson*, 194 F.3d 1149 (10th Cir. 1999); *Southeast Booksellers Ass'n v. McMaster*, 282 F. Supp. 2d 389 (D.S.C. 2003); *PSINet Inc. v. Chapman*, 167 F. Supp. 2d 878 (W.D. Va. 2001).

Each of the three Commerce Clause grounds found to invalidate the New York law challenged in *Pataki* applies with equal or greater force in this case. Here, the blocking orders under both the Statute and the Informal Notices have directly *halted* communications that would have otherwise taken place wholly outside of Pennsylvania (and indeed, although of arguably less constitutional significance, the blocking orders halted communications that would have otherwise taken place wholly outside of the United States). For example, the blocking actions taken by AOL to comply with the Pennsylvania Informal Notices affect AOL's entire *global* network, and thus halt communications that would have taken place entirely outside of Pennsylvania (and the U.S.). *See* AOL Dep. at 125-126. Similarly, the court order imposed on WorldCom under the Statute has directly obstructed communications on WorldCom's entire North American network. *See* WorldCom Dep. at 20.

[29] The *Pataki* court also squarely held what now seems almost obvious – that communications over the Internet do indeed constitute "commerce." *Id.* at 173 ("The inescapable conclusion is that the Internet represents an instrument of interstate commerce, albeit an innovative one; the novelty of the technology should not obscure the fact that regulation of the Internet impels traditional Commerce Clause considerations.").

Critically, the harm to non-Pennsylvania communications in this case is far greater than the burden found to be unconstitutional in *Pataki*. There, the New York law created a risk of criminal liability (under New York law) for a web publisher located outside of New York – thus, the Internet speech could take place, but the speaker might be hauled into the New York courts. In this case, however, the speech is *completely blocked* for non-Pennsylvania customers of ISPs that also operate in Pennsylvania. Well beyond merely "burdening" non-Pennsylvania speech, the blocking orders in this case halt the speech altogether.

Because the Statute and Informal Notices obstruct communications that would otherwise have occurred wholly outside of Pennsylvania, it is a *per se* violation of the Commerce Clause, and should be "struck down . . . without further inquiry." *Brown-Forman*, 476 U.S. at 579. *See also Healy*, 491 U.S. at 336; *Edgar*, 457 U.S. at 643; *Baldwin v. G.A.F. Seelig, Inc.*, 294 U.S. 511, 521 (1935).

B. The Statute and Informal Notices Are Invalid Because the Burdens They Impose Upon Interstate Commerce Exceed Any Local Benefit.

Moreover, the Statute and the Informal Notices cannot withstand a second Commerce Clause test, the balancing of local benefit against interstate harm. Again, the conclusion of the *Pataki* court is directly applicable to this case:

> Even if the Act were not a per se violation of the Commerce Clause by virtue of its extraterritorial effects, the Act would nonetheless be an invalid indirect regulation of interstate commerce, because the burdens it imposes on interstate commerce are excessive in relation to the local benefits it confers. The Supreme Court set forth the balancing test applicable to indirect regulations of interstate commerce in *Pike v. Bruce Church*, 397 U.S. 137, 142 (1970). . . . *Pike* requires a two-fold inquiry. The first level of examination is directed at the legitimacy of the state's interest. The next, and more difficult, determination weighs the burden on interstate commerce in light of the local benefit derived from the statute.

Pataki, 969 F. Supp. at 177. *See also Edgar*, 457 U.S. at 643-44 (state interests in protecting shareholders and regulating state corporations were insufficient to outweigh burdens imposed by allowing state official to block tender offers).

In this case, although the state interest in fighting child pornography is clearly legitimate, the enormous harm to interstate communications more than outweighs the minimal benefit that the Statute and Informal Notices provide. As detailed above in Section III.A, the challenged blocking orders have virtually no impact on the on-going operation of the child pornography industry, and do not significantly inhibit the ability of Pennsylvanians seeking access to child pornography to obtain such material. In contrast to this small benefit is the direct blocking of hundreds of thousands of web sites, directly preventing (for example) AOL users in all 49 other states from accessing a massive quantity of lawful and constitutionally protected content.

C. The Statute and Informal Notices Violate the Commerce Clause Because They Subject Interstate Use of the Internet to Inconsistent Regulations.

The Statute and Informal Notices are also precluded by the Commerce Clause because the lack of national uniformity created by conflicting state regulations of the Internet would impede the flow of interstate communications on the Internet. Once again, the *Pataki* analysis is directly applicable:

> Finally, a third mode of Commerce Clause analysis further confirms that the plaintiffs are likely to succeed on the merits of their claim that the New York Act is unconstitutional. The courts have long recognized that certain types of commerce demand consistent treatment and are therefore susceptible to regulation only on a national level. The Internet represents one of those areas; effective regulation will require national, and more likely global, cooperation. Regulation by any single state can only result in chaos, because at least some states will likely enact laws subjecting Internet users to conflicting obligations. Without the limitations imposed by the Commerce Clause, these inconsistent regulatory schemes could paralyze the development of the Internet altogether.

Pataki, 969 F. Supp. at 181. *See also Southern Pac. Co. v. Arizona ex rel. Sullivan*, 325 U.S. 761, 767 (1945) (state regulation of train length impeded the flow of interstate commerce). In this case, a number of other states have considered laws directly modeled on the Pennsylvania law challenged here,[30] as has the Council of State Governments as part of its "model state law" recommendation process. Although these efforts have to date been successfully thwarted, it is a certainty that if this Court upholds the Statute other states will follow Pennsylvania's lead. Thus, instead of ISPs being forced to comply with more than 500 blocking orders in this case (over an 18-month period), they might face *fifty* different sets of blocking orders, totaling tens of thousands of blocking orders nationwide. Entirely apart from the fact that the Internet would be brought to its knees in that scenario, the risk of multiple inconsistent sets of blocking orders like those in this case would directly threaten interstate commerce, and thus violates the Commerce Clause. The practical effect of fifty sets of blocking orders would be to "create just the kind of competing and interlocking local economic regulation that the Commerce Clause was meant to preclude." *Healy*, 491 U.S. at 337. Indeed, arguably, the dormant Commerce Clause precludes the entire field of online communications from state regulation because "the lack of national uniformity would impede the flow of interstate goods." *Exxon Corp. v. Governor of Md.*, 437 U.S. 117, 128 (1978) (retail market for gas did not preclude state regulation).

D. The Commerce Clause Arguments are Strongly Supported by Clear National Policy Preventing the Regulation of the Internet by Fifty Different States.

Although Plaintiffs are not asking this Court to decide – as suggested by the *Exxon Corp.* case – whether the dormant Commerce Clause should preclude the entire field of online communications from state regulation, there is strong support for such an outcome, and at a

[30] *See* Testimony of John B. Morris before the Judiciary Subcommittee of the Maryland House of Delegates,

minimum that support should encourage this Court to declare that Internet regulation of the type challenged here violates the Commerce Clause.

The United States Congress has repeatedly decided that to the extent there should be any governmental regulation of the Internet, it should be done on a national basis, not a state-by-state basis. As recently as this week (specifically, on Dec. 8, 2003), the Congress enacted major legislation addressing the problem of unsolicited e-mail (or "spam"), and a key element of that bill is the federal preemption of state laws aimed at reducing spam.[31] Similarly, Congress has acted to expressly preempt or prohibit state-by-state regulation in the areas of, for example, taxation[32] and financial privacy.[33]

But most relevant to the case now before the Court is the express declaration by the U.S. Congress that ISPs should not be liable for content posted by others elsewhere on the Internet. Specifically, the Statute challenged here is in direct tension with Section 230 of the Telecommunications Act of 1996, 47 U.S.C. § 230, which makes clear that states should not hold ISPs liable for content that is merely *accessible through* the ISP:

> No provider or user of an interactive computer service [i.e., an ISP] shall be treated as the publisher or speaker of any information provided by another information content provider [i.e., a website].

47 U.S.C. § 230(c)(1).[34] Thus, under the system established by Congress in 1996 (and upheld and enforced by numerous courts across the country), the legal responsibility for content on the Internet lies with the individuals or entities that publish the content on the Internet, and not with

---

March 4, 2003, regarding Maryland House Bill 661.

[31] *See* S. 877 (108th Cong.), "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003."

[32] *See* Internet Tax Nondiscrimination Act of 2001, Public Law 107-75.

[33] *See* 15 U.S.C. §§ 6801-6809 (Gramm Leach Bliley Act).

[34] Section 230(c)(3) expressly preempts any state laws that conflict with Section 230(c)(1).

ISPs through whose networks the content can be accessed. Although addressing state law tort liability, the analysis of the leading case interpreting Section 230 is relevant to the case now before this Court:

> The purpose of this statutory immunity is not difficult to discern. Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium. The imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech. Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum. In specific statutory findings, Congress recognized the Internet and interactive computer services as offering "a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity." *Id.* § 230(a)(3). It also found that the Internet and interactive computer services "have flourished, to the benefit of all Americans, *with a minimum of government regulation*." *Id.* § 230(a)(4) (emphasis added). Congress further stated that it is "the policy of the United States . . . to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, *unfettered by Federal or State regulation*." *Id.* § 230(b)(2) (emphasis added).

Zeran v. America Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997) (emphasis in original). Although the Court does not need to resolve whether the Statute challenged here treats ISPs as a "publisher" or "speaker" (and thus would clearly be preempted by § 230), Section 230 provides very strong evidence of the approach that the U.S. Congress has adopted for the Internet, and that national policy in turn supports the conclusion that the Statute and Informal Notices must fall under the analysis of the Commerce Clause of the U.S. Constitution.

CONCLUSION

For the myriad reasons set out above – not the least of which is the 600,000-plus web sites that are blocked today – this Court should declare both the Statute and the Informal Notices to be unconstitutional and without legal force or effect, and should enjoin their enforcement.

Respectfully Submitted,

_____

John B. Morris, Jr., Esq.
Lara M. Flint, Esq.
Center for Democracy & Technology
1634 I Street, NW, Suite 1100
Washington, D.C. 20006
(202) 637-9800

_____

Stefan Presser, Esq.
Bar No. 43067
Legal Director
American Civil Liberties Union
of Pennsylvania
125 South Ninth Street
Suite 701
Philadelphia, PA 19107
(215) 592-1513 ext. 116

Seth Kreimer, Esq.
Bar No. 26102
3400 Chestnut Street
Philadelphia, PA 19104
(215) 898-7447

Dated: December 12, 2003