IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

CENTER FOR DEMOCRACY & TECHNOLOGY, et al,	:	CIVIL ACTION
	:	
v.		
	:	
GERALD J. PAPPERT, ACTING ATTORNEY GENERAL OF PENNSYLVANIA	:	NO. 03-5051

ORDER

AND NOW, this day of January, 2004, it is ORDERED that

1. Plaintiffs' Motion for Declaratory Relief and Preliminary and Permanent Injunctive Relief is DENIED;

2. The Preliminary Injunction entered September 9, 2002 is VACATED;

3. Judgment is entered in favor of Defendant and against Plaintiffs.

BY THE COURT:

_____
JAN E. DUBOIS, J.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

CENTER FOR DEMOCRACY & TECHNOLOGY, et al,	:	CIVIL ACTION
	:	
v.		
	:	
GERALD J. PAPPERT, ACTING ATTORNEY GENERAL OF PENNSYLVANIA	:	NO. 03-5051

DEFENDANTS' BRIEF IN OPPOSITION TO PLAINTIFFS' MOTION FOR DECLARATORY RELIEF AND PRELIMINARY AND PERMANENT INJUNCTIVE RELIEF

GERALD J. PAPPERT
ACTING ATTORNEY GENERAL

BY:
John O.J. Shellenberger
Chief Deputy Attorney General
Identification No. 09714

OFFICE OF ATTORNEY GENERAL
21 S. 12th Street, 3rd Floor
Philadelphia, PA 19107-3603
Telephone: (215) 560-2940
Fax: (215) 560-1031

TABLE OF CONTENTS

Table of Contents (Continued)

Table of Contents (Continued)

STATEMENT OF THE CASE

In February 2002, Pennsylvania enacted a statutory procedure to authorize interference with the distribution of illegal child pornography through the Internet, thereby combating the sexual exploitation and abuse of children inherent in child pornography. The statute requires an Internet Service Provider (ISP) (an entity that enables its users to access content offered over the Internet) to remove child pornography items residing on its services or disable access to child pornography items accessible through its services (and accessible to persons in Pennsylvania) after a court authorizes removal or disablement and the Attorney General notifies the ISP of the court's authorizing order.

This action has been brought by two organizations (Center for Democracy & Technology (CDT) and the American Civil Liberties Union of Pennsylvania (ACLU)) and an alleged ISP (Plantagenet, Inc.).[1] They seek to have a significant portion of the law, and the Pennsylvania Attorney General's sensible informal means of implementing it, declared unconstitutional and enjoined. They have named the Attorney General as the defendant.[2]

---

[1] In the latter plaintiff's corporate papers, the name is written PlantagaNet, Inc.

[2] When this action was filed, D. Michael Fisher was the Attorney General of Pennsylvania. He has since been appointed to the federal bench, and Gerald J. Pappert has been appointed Acting Attorney General. Mr. Pappert is automatically substituted as defendant here under Fed.R.Civ.P. 25(d)(1).

In response to a Motion for a Temporary Restraining Order filed with the Complaint, the Attorney General suspended his process of informally requesting ISPs to remove or disable access to child pornography. He agreed to a preliminary injunction against issuance of the informal notices by which his staff had been making the requests.

Plaintiffs have now filed a Motion for Declaratory Relief and Preliminary and Permanent Injunctive Relief asking the Court to declare the statute and the informal notice process unconstitutional, enjoin the Attorney General from issuing any more informal notices, enjoin the Attorney General from taking any action against any ISP for failing to comply with an informal notice issued in the past, and order the Attorney General to send a copy of the Court's injunctive order to each ISP that has received an informal notice.

The Defendant Attorney General opposes the new Motion and asks that the Court vacate the previously entered preliminary injunction. Defendant contends that neither the statute nor the informal notice process violates the First Amendment, the Commerce Clause, or any other federal law. In brief, Defendant contends:

! Plaintiffs do not challenge, but actually endorse, a significant part of the statute.

! Neither the statute nor the informal notices, by their terms, require any ISP to perpetually disable its customers' access to any Internet location, address, or identifier after it no longer provides access to a child pornography item, but even if they did, they would not materially or illegally restrain speech.

! The statutory procedures do require an adversary hearing at which the State must prove that the items it has identified are child pornography before

any adverse action may be taken or threatened against an ISP for failing to disable access to the items.

! The procedures provided by the statute even before the initial court order of authorization meet the needs of the First and Fourteenth Amendments where the issue for determination is child pornography.

! The informal notice procedure need not comply with constitutional procedures because it is an informal non-coercive process.

! The informal notice procedure does comply with constitutional procedures because, as with the statute, the issue for determination is child pornography.

! Neither the statutory nor informal notices intentionally restrain any constitutionally protected speech by their terms and do not unintentionally restrain constitutionally significant amounts of speech as any necessary result of Internet technology. ISPs can disable access to child pornography items likely to be identified in Defendant's notices without disabling access to any significant amount of legitimate speech.

! Neither the statutory nor informal notices violate the dormant Commerce Clause because child pornography is not commerce and because the effect of the notices on legitimate commerce neither discriminates against interstate commerce nor significantly burdens interstate commerce.

STATEMENT OF THE FACTS

The parties will submit a joint Statement of Uncontested Facts. The parties will also submit their own proposed findings of fact as to the facts that are disputed. These submissions will provide the full factual background, both accepted and contested. A brief summary follows.

On February 21, 2002, Pennsylvania adopted a new statute regarding child pornography on the Internet, effective April 22, 2002. It is now found at 18 Pa.C.S. §§ 7621-7630 in a subchapter titled "Internet Child Pornography." The statute permits the Attorney General or a district attorney to apply to a common pleas court for an order (1) finding probable cause that a specified item residing on or accessible through an ISP's services is child pornography as defined at 18 Pa.C.S. § 6312 and (2) authorizing the Attorney General to notify the ISP upon whose services the item resides or through whose services the item is accessible to remove the item or disable access to it. 18 Pa.C.S. § 7626. If the court issues the order and the Attorney General gives the notice, but the ISP does not comply within five business days after the notice, the Attorney General or district attorney may charge the ISP with a crime. 18 Pa.C.S. §§ 7622, 7624.

Before the new law's effective date, several large ISPs, the ISPs' trade association, and Office of Attorney General (OAG) representatives met and all decided that they would like the Attorney General to use an informal method of notifying ISPs of child pornography items before filing court applications and

issuing notices of court orders. The OAG staff drafted a form of informal notice, which was later revised.

After the law's effective date, OAG agents both reviewed citizen complaints of child pornography on the Internet and searched the Internet on their own for child pornography. When they determined that sites displayed child pornography, they sent informal notices to the ISPs through whose services the offending material had been accessed, asking the ISPs to disable their subscribers' access to the sites. The sites were identified by their Uniform Resource Locators, or "URLs" (*e.g.* http://www.example.com), through which the child pornography could be accessed. The notices did not instruct the ISPs how they were to disable access. The ISPs generally wrote in response that they had complied with the notice. These informal notices and responses continued until September 9, 2003, when this action was filed and the Court entered the preliminary injunction enjoining the informal notices.

In July 2002, one ISP, WorldCom, informed the OAG that it would only disable access in response to a court order. In September 2002, the Attorney General obtained a court order finding probable cause that five items that had been accessed through WorldCom's services were child pornography. The Attorney General then notified WorldCom to remove or disable its subscribers' access to the items, identified by their URLs. WorldCom responded in writing that it had complied with the notice.

Other than the court application regarding WorldCom, neither the Attorney General nor any district attorney has filed any other court application under the statute. The OAG has sent no informal notices to WorldCom since July 2002.

At the pre-effective date meetings, the ISPs and the OAG staff also discussed methods of disabling access to sites that did not reside on the ISPs' services. The OAG staff said that access could be disabled, or blocked, by making entries in equipment known as domain name servers. These entries, in effect, stop all requests for the site because they stop requests for the full domain name, or hostname, of the site, that is, www.example.com or www.badsite.example.com. The parties also discussed a method of blocking IP addresses associated with the sites' URLs. The IP address is a number that identifies for Internet purposes where the site can be found.

In discovery in this action, several ISPs (America Online, Comcast, and WorldCom as to two of the URLs identified in the court authorized notice) have said that they disabled access to the child pornography items by blocking the IP addresses associated with the URLs through which the items were accessed. Because more than one site can be assigned to a single IP address, and blocking the IP address blocks access to all the sites that use it, use of this method probably blocked more sites than those actually targeted.

Some ISPs have said that they disabled access by making entries in their domain name servers (Verizon, Epix). These entries stopped requests for the

full domain name, or hostname, of the site. The entries did not block access to any URL that did not use the same full domain name. They did block access to all pages under the domain name, such as www.example.com/yyyy and www.example.com/zzzz. Blocking sub-pages did not generally block access to any independent content, except in the situation of "online communities" that permit the posting of independent content as sub-pages under their domains.

By mid-September 2002, OAG staff had become aware that disabling access to an online community's domain name disabled access to independent content residing on sub-pages under it. In early October 2002, the OAG staff decided that where they could determine that the site was this kind of online community, they would go directly to the administrators of the community and ask them to remove the offending content from their service. The OAG staff would not send an informal notice to the ISP through which the site was accessed. The OAG continued this practice until September 9, 2003, when it terminated these online community contacts because it thought that the preliminary injunction might be read to prohibit them.[3]

---

[3] As Plaintiffs note, an OAG agent contacted directly the operator of a web site, which might have been some kind of online community, as early as April 2002. If necessary, the agent will explain that he did so then because it was an atypical case. In an exercise of caution, he felt that direct contact, if possible, would be useful. He was able to make the contact and resolved the issue. He reported the case to the National Center for Missing and Exploited Children, the national clearinghouse for child pornography information.

Also, if Plaintiffs' assertions are correct, the agents once in 2003 did not recognize an online community and sent an informal notice to the ISP through which the offending community page had been accessed. The ISP then blocked

(continued...)

Upon occasion, ISPs contacted entities that hosted sites identified in informal notices. When the OAG notified WorldCom of the court order, the covering letter noted that if any of the sites resided on a web hosting service, and WorldCom could get the service to remove the site from its services, that would constitute compliance. WorldCom's response stated that in three of the cases identified in the notice, it had contacted the sites' hosting services and they removed the sites from their services.

Plaintiffs' expert says that today IP address blocking and domain name server entries are methods ISPs can use to disable their subscribers' access to sites that do not reside on the ISPs' services. However, he says that IP address blocking is the more effective method of preventing access to the offending sites. He concedes that IP address blocking will in many cases block access to many non-targeted sites.

Defendant's expert says that domain name server entries are a cost-efficient, technologically simple, and reasonably effective method of disabling access to the offending sites and pose little risk of disabling access to non-targeted sites. He also says that other effective and even better focused methods are technologically available, although they would probably be costly and complicated for many ISPs at this time.

---

[3](...continued)
access to the entire online community. Defendant would go to the community now and ask that it remove the page (as the ISP could also do), but fears that such a contact might be considered an informal notice prohibited by the preliminary injunction.

ARGUMENT

I. PLAINTIFFS CDT AND ACLU HAVE STANDING TO PURSUE ONE CLAIM; OTHERWISE, PLAINTIFFS LACK STANDING.

At most only two of the plaintiffs can establish standing as to one of their claims. Plaintiff Plantegenet, Inc. lacks standing to sue at all. Plaintiff CDT may have standing as an alleged receiver of speech and plaintiff ACLU may have standing as an organization some of whose members are alleged receivers of speech to challenge procedures used to determine child pornography. But they do not have standing to challenge either the statute or the informal notice process insofar as the claims depend on decisions of the ISPs.

A plaintiff may not sue for declaratory or injunctive relief unless it has standing. This requires at minimum that the plaintiff and its claim present a case or controversy recognized as justiciable under Article III, § 2 of the Constitution. To establish a justiciable case or controversy, a plaintiff must prove that it has suffered, is suffering, or is in imminent danger of suffering a real injury in fact. The injury must be caused by the allegedly illegal conduct of the defendant, and the court must be able to redress or prevent the injury. *Steel Co. v. Citizens for a Better Environment,* 523 U.S. 83, 102-104 (1998); *Lujan v. Defenders of Wildlife,* 504 U.S. 555, 560, 561 (1992); *Babbitt v. United Farm Workers,* 442 U.S. 289, 298 (1979). Standing focuses on who may sue, and emphasizes that plaintiffs may only pursue their own claims, not those of others. *Warth v. Seldin,* 422 U.S. 490, 499, 502, 514 (1975).

Plaintiff Plantagenet, Inc. lacks standing. While the Complaint alleges that it is an ISP that might receive a notice of court order under the statute or an informal notice from Defendant's staff, in truth it is such an insignificant operation that it is hardly an ISP. At least, the likelihood of any notice is too small to support a case or controversy. According to answers to interrogatories, Plantagenet has one employee. Answer to Interrogatories 8, 9. It does not own or operate the equipment that a real ISP would own and operate, *e.g.* access lines, modems, routers or other equipment customers of an ISP use to access the Internet. Answer to Interrogatory 11. Whatever service it provides, it has only 750 to 800 customers. Answer to Interrogatory 12.

While the statute in question here defines Internet Service Provider broadly, and Plantagenet might barely fall within it, its tiny customer base means that Defendant would never proactively subscribe to its services.[4] Disabling access to child pornography through Plantagenet would have too little impact on child sexual abuse. Likewise, no citizen will likely complain to Defendant about child pornography accessed through Plantagenet because so few citizens use Plantagenet's services. Moreover, Defendant will not likely consider an entity that does not even own ISP equipment to be an ISP. Defendant will go to the ISP that does own the equipment and can disable access. "Persons having no fears of state prosecution except those that are

[4] The statute defines "Internet Service Provider" as "A person who provides a service that enables users to access content, information, electronic mail or other services offered over the Internet." 18 Pa.C.S. § 7621.

imaginary or speculative, are not to be accepted as appropriate plaintiffs." *Younger v. Harris,* 401 U.S. 37, 42 (1971).

Plaintiffs claim that Plantagenet can assert the rights of its customers. However, Plantagenet's customers will only be affected if Plantagenet gets a notice, statutory or informal, to disable access to a site. If notices to Plantagenet are too unlikely to threaten it with injury, its customers are at no risk of injury either. Moreover, a party has no standing to assert the rights of others unless it is suffering an actual injury itself, the plaintiff and the other parties have a close relationship, and the other parties are unable to protect their own interests. *The Pitt News v. Fisher,* 215 F.3d 354, 362 (3d Cir. 2000). Here, Plantagenet is not suffering an actual injury itself.

Plaintiffs CDT and ACLU claim standing as receivers of speech, not as speakers. The ACLU further claims to represent its members as receivers of speech. While persons have a First Amendment right to receive protected speech, *Virginia St. Bd. of Pharmacy v. Va. Citizens Council,* 425 U.S. 748, 756, 757 (1976), they can only have standing to assert the right if the Defendant is likely to deprive them of protected speech that they wish to receive.

Plaintiffs cannot assert First Amendment "overbroadness" standing. This kind of standing only affords standing to speakers to facially challenge statutes that expressly restrain speech. It gives a plaintiff standing to attack an allegedly overbroadly worded statute even if the plaintiff's own speech could have been "regulated by a statute drawn with the requisite specificity."

Broadrick v. Oklahoma, 413 U.S. 601, 612 (1973), *quoting Dombrowski v. Pfister,* 380 U.S. at 486. "An individual whose own speech or expressive conduct may validly be prohibited or sanctioned is permitted to challenge a statute on its face because it also threatens others not before the court." *Brockett v. Spokane Arcades, Inc.,* 472 U.S. 491, 503 (1985); s*ee also New York v. Ferber,* 458 U.S. 747, 768, 769 (1982).[5] This kind of standing does not permit just anyone to challenge a statute because it might restrain speech that someone else would like to receive. It does not give an alleged receiver of speech standing to assert the rights of a speaker whose speech the plaintiff had no particular desire to receive. It does not apply where the law allegedly has overly broad effects rather than overly broad language. That is, it does not apply when the literal scope of the law does not potentially chill expression of persons not before the court.

Here, Plaintiffs do not claim that the language of the statute is overbroad. They do not claim that the scope of the statutory language, by its very existence, chills speech. They are not speakers whose speech might be covered by the law, properly or not. Overbroadness standing doesn't apply in this case.

CDT claims to receive Internet access from a major ISP, MCI (formerly WorldCom). WorldCom received a notice of court order under the statute in

---

[5] For example, the plaintiffs in *Ashcroft v. Free Speech Coalition,* 122 S.Ct. 1389 (2002) were producers of erotic materials that could have fallen within the prohibitions of the federal statute as it was worded. Therefore, they were permitted to challenge the statute on its face.

September 2002, and it might conceivably receive one again some day. The ACLU receives its Internet access from an ISP that has never received a notice of court order or an informal notice from Defendant. Whether it ever will is a matter of speculation. However, the ACLU says that associations like it may sue on behalf of their members if the members would have justiciable claims in their own right, *Warth v. Seldin,* 422 U.S. at 511; *Pennsylvania Psychiatric Society v. Green Spring Health Services, Inc.,* 280 F.3d 278, 283 (3d Cir. 2002). The ACLU claims that some of its members access the Internet through major ISPs, some of which have received informal notices and will likely receive more in the future. However, the possibility that a plaintiff's ISP will receive a notice is not enough to afford the plaintiff standing, either on its own or through an association.

Perhaps Defendant's actions under the statute or the informal notice process could arguably, in some remote instance, cause CDT and the ACLU members to be deprived of child pornography-like material that a judge or law enforcement officer might mistake for child pornography. In this light, perhaps these plaintiffs have standing to challenge the procedures employed under the statute and the informal process to determine child pornography.

However, Defendant has not caused and will not cause deprivation of access to web sites not identified in the notices and not representing child pornography items. Plaintiffs lack standing to challenge the statute and informal notice procedure insofar as the challenge depends on decisions by the

ISPs. The notices identify only sites that allegedly contain child pornography and identify them only by their specific URLs at the time of the notice. The notices do not request disablement of access to any other sites. They do not suggest a method of disabling access to the sites identified. The ISP selects the method. If the method causes disablement of access to other sites, the ISP has caused it. "When the plaintiff is not himself the object of the government action or inaction he challenges, standing is not precluded, but it is ordinarily 'substantially more difficult' to establish." *Lujan,* 504 U.S. at 562. The plaintiff must show that the regulated person's choices will of necessity be made in a manner that causes injury to the plaintiff, injury that can be redressed by a judgment against the government defendant. *Id.*

Even if Defendant's actions can be found to cause disablement of access to sites other than those identified in Defendant's notices, Plaintiffs have no standing unless they, or their members, actually will want to access those other sites. Whether they do, whether they will, are matters of speculation. All the ACLU members have said is that when they search the World Wide Web, they want as broad a search as possible. Verifications of Clark Moeller, Janet Goldwater, Gene Bishop, Dana Devon. Whether their searches will be meaningfully narrowed by anything the ISPs have done is a matter too speculative to support standing.

II. PLAINTIFFS DO NOT CHALLENGE THE STATUTE INSOFAR AS IT PERMITS COURT ORDERS AND NOTICES OF COURT ORDERS DIRECTING INTERNET SERVICE PROVIDERS TO REMOVE CHILD PORNOGRAPHY RESIDING ON THEIR SERVICES.

Plaintiffs do not really challenge one feature of the Pennsylvania statute; indeed, they implicitly applaud it. The Court should leave it intact.

Again, the statute in question is found at 18 Pa. C.S. § 7621-7630. At § 7622, it provides:

> Duty of Internet service provider
>
> An Internet service provider shall remove or disable access to child pornography items residing on or accessible through its service in a manner accessible to persons located within this Commonwealth within five business days of when the Internet service provider is notified by the Attorney General pursuant to § 7628 (relating to notification procedure) that child pornography items reside on or are accessible through its service.

18 Pa. § 7622. The statute further authorizes either the Attorney General or a district attorney to apply to a Common Pleas Court for an order of authorization "to remove or disable items residing on or accessible through an Internet service provider's service." 18 Pa. § 7626. If the Court enters the order, the Attorney General is to provide the ISP identified in the application with copies of the application and the Order and notify the ISP that it "must remove or disable the items residing on or accessible through its service within five business days of receipt of the notification." 18 Pa. C.S. § 7628.

Thus, the orders and notices issued under the statute can impose two kinds of obligations on ISPs. The orders and notices can direct an ISP to

remove or disable access to child pornography items "residing on" its service. The orders and notices can direct an ISP to disable access to child pornography items "accessible through" its services. Plaintiffs in this case attack the latter kind of order and notice, not the former.

Plaintiffs really perceive constitutional problems only where the court order and notice are directed to an ISP that does not host the offending site, that is, where the offending site does not reside on its services, but resides elsewhere, and can only be accessed through the ISP's services. Then, Plaintiffs allege, the disabling actions the ISP will take will prevent its customers' access to non-offending sites. Then, a particular URL may remain inaccessible through the ISP even if the content it represents changes. Defendant contests this claim too, but this claim does not affect that portion of the statute that permits court orders and notices directing ISPs to remove child pornography items that *reside on* their services.

When ISPs remove offensive sites from their services, they cannot possibly interfere with access to other sites. Plaintiffs themselves argue that ISPs can easily remove web sites residing on their services or their servers if the sites display child pornography, without interference with any web sites that do not display child pornography. Complaint ¶ 88; Memorandum in Support of Plaintiffs' Motion, pp. 37-39. ISPs agree. *Id.* Indeed, Plaintiffs contend that government *should* attack child pornography on the Internet by contacting the

hosting ISPs, that is, the ISPs upon whose services the offending sites reside. *Id.;* Complaint, ¶ 90.[6]

Thus, the Court must at least leave the statute intact and untouched insofar as the statute authorizes orders and notices directing an ISP to remove child pornography items residing on its services. If this holding requires severance of the "residing on" provision from the "accessible through" provision, the Court should sever. *See Brockett v. Spokane Arcades, Inc.,* 472 U.S. 491, 504-507 (1985). The severability of state laws is a matter of state law, and Pennsylvania law favors severability. *Planned Parenthood of Southeastern Pennsylvania v. Casey*, 978 F.2d 74, 77, 78 (3d Cir. 1992); *see also Sullivan v. Barnett*, 139 F.3d 158, 173 (3d Cir. 1998), *rev'd. on other grounds,* 526 U.S. 40 (1999); *Contractors Association v. City of Philadelphia,* 6 F.3d 990, 996, 997 (3d Cir. 1993). Indeed, under Pennsylvania law, "the provisions of every statute shall be severable." 1 Pa. C.S. § 1925. Certainly here, the two statutory provisions can easily be separated, as Plaintiffs separate the two concepts. Thus, Section 7622 would effectively read:

> An Internet service provider shall remove or disable access to child pornography items residing on its service in a manner accessible to persons located within this Commonwealth within five business days of when the Internet service provider is notified by the Attorney General pursuant to section 7628 (relating to notification procedure) that child pornography items reside on its service.

Subsequent sections of the statute would be adjusted similarly.

---

[6] Plaintiffs appear to recommend that the government contact the source of the child pornography with or without a court order. Complaint ¶ 90.

III. NEITHER THE STATUTE NOR THE INFORMAL NOTICES CREATE AN ONGOING PRIOR RESTRAINT OF SPEECH, BUT EVEN IF THEY DO, THE MINIMAL RESTRAINT VIOLATES NO CONSTITUTIONAL PROVISION.

Pennsylvania's Internet Child Pornography Law is valid on its face. It does not require disablement of access to any web site that has First Amendment protection. The statutory procedures require disablement of access only to sites that display child pornography -- "child pornography items." The First Amendment does not protect child pornography. Disablement of access to it violates no one's First Amendment rights.

The law clearly and narrowly defines the material that it seeks to suppress: child pornography. It is defined at 18 Pa.C.S. § 6312, and Plaintiffs do not contest the definition. The definition is consistent with state laws that the Supreme Court has upheld. *New York v. Ferber,* 458 U.S. 747, 751 (1982); *Osborne v. Ohio,* 495 U.S. 103, 106, 107, 112-114 (1990). It is also consistent with the federal Criminal Code's definition, including the age that defines "child" (18 years). 18 U.S.C. § 2256.

Plaintiffs argue that the statute, and also the informal notices, create an inherent ongoing prior restraint of speech by preventing any future use of a particular URL or IP address. They misread the statute, but even if their reading were right, the effects on speech would be too small to implicate the First Amendment, and the restriction on the URL's use would be constitutionally justified.

A. The statute does not require perpetual disablement of access to any URL or IP address.

The statutory procedures do not prohibit use of URLs or IP addresses at all. The heart of the statute, § 7622, provides only that an ISP "shall remove or disable access to *child pornography items* residing on or accessible through its service." (emphasis supplied). The statute nowhere mentions IP addresses. Section 7626(4) does require that the application to the court contain, "the Uniform Resource Locator providing access to the items," but the concern is with the items; the URL is just the access to them. The Attorney General's notice, described at § 7628, is to require removal or disablement of "the items," although presumably, and necessarily, it will identify them by the URL through which they are accessible. That is, the notice must state the URL, but the URL has meaning only with the child pornography item to which it provides access at that time.

If the ISP finds the item *residing on* its own services, it removes it, presumably along with its URL. However, nothing prevents the URL from re-use anytime. The IP address is unaffected.

If the item is only *accessible through* the ISP's services, the ISP could use the URL to begin a process to find the item's host and then ask the host to remove the item from its services or servers. The URL would be down temporarily, but could be re-used.

The ISP could also disable its customers' access to the URL identified in the notice through some "blocking" or "filtering" method. In the event of

blocking, the ISP's customers would not be able to access anything through the URL. However, once that URL no longer provides access to the child pornography item, the statute no longer requires that the ISP block or disable access to the URL. True, the statute does not give directions for unblocking. Unblocking perhaps requires communication between the ISP and the Office of Attorney General. But the statute does not require continued disablement.

Blocking the IP address goes far beyond the statutorily required "child pornography item." But even if an ISP has to block the IP address, again, the statute does not require that the ISP block it (disable access to it) if a child pornography item does not reside under it. Those ISPs that are blocking an IP address when even the URL that started it no longer resides at that address, should stop.

The informal notices can require no more than the statutory notices. Indeed, they require less, for they do not even require the initial disablement of access to the URL, much less maintenance of it after the child pornography is no longer accessible through the URL. Again, the ISP and the OAG may need to communicate, but that communication can come from either end.

B. Even if the statute does require perpetual disablement of access to a URL, that disablement does not restrict speech.

Even if the statute required continued disablement of an ISP's customers' access to a URL, it would not violate the Constitution. No particular URL is needed to exercise First Amendment rights. A URL is not like the persons enjoined from publishing any malicious, scandalous, or defamatory newspaper

described in *Near v. Minnesota,* 283 U.S. 697 (1931).[7] A URL is not like the community organization that was enjoined from passing out any literature and picketing anywhere in an Illinois city, as involved in *Organization for a Better Austin v. Keefe,* 402 U.S. 415 (1971). A URL is not like the movie theater that was not allowed to show any movies, as was of concern in *Vance v. Universal Amusement Co.,* 445 U.S. 308 (1980). In those cases, the speech restraints were applied either to actual people or to real physical forums of which only a limited number can exist in a community. Without the people or the forums, speech was surely diminished.

A URL is neither a person, nor a real forum, nor a limited commodity. It is a little string of letters and numbers that acts as a superficial label. URLs are infinite in quantity. Even complete retirement of one will not diminish speech. Speech can always find another URL, and probably pretty close to the out-of-commission string. The new URL will be in the same cyber-space, accessible in the same physical places, as the retired URL. It can relate to the same IP address, which is the true computer address. Disablement of an ISP's customers' access to a particular URL for even an indefinite time does not implicate First Amendment rights.

---

[7] At page 27 of their Memorandum, Plaintiffs write as if the injunction in *Near* was against use of a particular name, The Saturday Press. Instead, the injunction enjoined a group of people from publishing any newspaper, no matter what its name, that contained malicious, scandalous, or defamatory matter. 283 U.S. at 706.

C. Even if the statute requires perpetual disablement of access to a URL, and even if that disablement restricts speech, it does not violate the Constitution.

Even if a statutory or informal notice does require disablement of access to a URL after the child pornography has left it, and even if that implicates First Amendment rights, it is justified if the URL once provided access to child pornography items. The Supreme Court has upheld laws that destroy speech forums and materials because they have in the past been associated with illegal activity. In *Aracara v. Cloud Books,* 478 U.S. 697 (1986), the Court upheld a state statute that authorized closure of a public building that had been used for prostitution and lewdness, even though the building housed a bookstore. The closure sanction was directed at unlawful conduct, not expressive activity. The order could not be considered a prior restraint because the booksellers were free to carry on their bookselling business at another location, even though other locations might be scarce. 478 U.S. at 705, n.2. Similarly, in *Alexander v. U.S.,* 509 U.S. 544 (1993), the Court upheld forfeiture of an entire adult entertainment business, including much First Amendment protected material, based on the owner's convictions for selling seven obscene items.

Even if the statute here did require long term disablement of access to a particular URL, the fact that the URL once provided access to child pornography would justify the disablement. Child pornography is illegal in Pennsylvania as in other states and under federal law. 18 U.S.C. §§ 2252,

2252A, 2256; *see* attached appendix of state laws. It is illegal because it is the incarnation of sexual abuse of children. *New York v. Ferber,* 458 U.S. 747 (1982); *Osborne v. Ohio,* 495 U.S. 103 (1990). Once attached to this criminal activity, its Internet identifier, its Internet point of accession, should be substantially retired to prevent it from performing this nefarious service again.

IV. THE STATUTE DOES NOT VIOLATE ANY PROCEDURAL REQUIREMENTS BECAUSE THE PROCEDURES EMPLOYED RENDER DETERMINATIONS OF CHILD PORNOGRAPHY WITH CONSTITUTIONALLY SUFFICIENT ACCURACY.

Again, Pennsylvania's Internet Child Pornography Law is valid on its face. It does not require disablement of access to any web site that has First Amendment protection. The statutory procedures require disablement of access only to child pornography items. The law clearly and narrowly defines child pornography consistent with state laws that the Supreme Court has upheld, *New York v. Ferber,* 458 U.S. 747, 751 (1982); *Osborne v. Ohio,* 495 U.S. 103, 106, 107, 112-114 (1990), and consistent with the federal Criminal Code. 18 U.S.C. § 2256.

Plaintiffs contend that the statute violates the First and Fourteenth Amendments because it does not require an adversary judicial proceeding with findings based on something more than probable cause, a procedure deemed constitutionally necessary before government attempts to suppress material it claims is obscene (to determine whether the material really is obscene). However, the statute under consideration here does provide for an adversary judicial proceeding before government sanctions apply to anyone. Moreover,

the statute here does not deal with obscenity. It deals with child pornography, and the Constitution does not require the procedures to which Plaintiffs point when the determination to be made is child pornography. That is, a court acting *ex parte* (as the Pennsylvania law permits at the initial proceeding) can make a sufficiently accurate determination of whether particular visual depictions are or are not child pornography without an adversary judicial proceeding. Furthermore, a finding of probable cause to believe that an item is child pornography is effectively a finding that the item is child pornography.

Because Plaintiffs CDT and ACLU assert standing only as receivers of allegedly protected speech, not as creators of speech, they have a weak interest in accurate determinations of child pornography. Even if judges, or law enforcement officers, occasionally identify material as child pornography that is not really child pornography, Plaintiffs still will not likely have much interest in it. Moreover, the error will affect Plaintiffs' access to only one web site (and only through a limited number of ISPs). They will be able to access other sites that display similar near, but not quite, child pornography.

A. The Statute here, read in light of the Supreme Court decision in *McKinney v. Alabama*, 424 U.S. 669 (1976), provides an adversary judicial proceeding before the government threatens or imposes any sanctions for failure to suppress a web site as child pornography.

To assure accurate determinations and prevent suppression of protected speech, government generally may not suppress expressive material as obscene without first giving the speaker or distributor an opportunity for an adversary judicial proceeding and a finding of obscenity based on at least the

preponderance of the evidence. *See Fort Wayne Books, Inc. v. Indiana,* 489 U.S. 46 (1989); *Blount v. Rizzi,* 400 U.S. 410 (1971); *Freedman v. Maryland,* 380 U.S. 51 (1965); *Marcus v. Search Warrants*, 367 U.S. 717 (1961)*; Kingsley Books v. Brown,* 354 U.S. 436 (1957). These holdings have been based on the First Amendment and procedural due process. Even if the First Amendment or Due Process Clause also requires an adversary judicial proceeding before an item can be suppressed as *child pornography*, the statute here, read in light of the Supreme Court decision in *McKinney v. Alabama,* 424 U.S. 669 (1976), does provide such a proceeding before imposition of the statutory sanction. This proceeding suffices to sustain the statute.

The initial court proceeding and order, which may be *ex parte* and based on probable cause, do not impose any obligations on an ISP and do not authorize the Attorney General or district attorney to do anything other than issue a notice to the ISP. This initial order only advises the Attorney General or district attorney that the web sites identified constitute probable cause evidence of a violation of 18 Pa.C.S. § 6312 (defining child pornography) and that such items shall be removed or disabled from the ISP's service. 18 Pa.C.S. § 7627.

The entry of the initial order authorizes the Attorney General to notify the ISP of the order and to direct the ISP to remove or disable access to the web site identified within five business days after receipt of the notice. 18 Pa.C.S.

§ 7628. However, this notice is not to contain any threat of, or even reference to, prosecution. § 7628(c).

If the ISP fails to implement the notice, the Attorney General or district attorney may then charge the ISP with a crime. 18 Pa.C.S. § 7624. The statute authorizes no other sanction against an ISP.

The statute does not provide that the prior finding of probable cause of child pornography is binding in any criminal prosecution. Indeed, the statute's authorization of the preliminary order on probable cause, and its definition of that order as merely an order authorizing the Attorney General to give notice, indicate that the ultimate determination of child pornography (*i.e.,* violation of 18 Pa.C.S. § 6312) is for the criminal trial.

A criminal prosecution must be accompanied by all the protections constitutionally required in a criminal prosecution, the highest form of procedural due process. The Supreme Court, in *McKinney v. Alabama,* 424 U.S. 669 (1976), held that a prior determination that materials were obscene cannot bind a person who is criminally prosecuted for selling the materials when he was not a party to, and had no notice of, the proceeding at which the determination was made. He has the right to litigate the issue of obscenity in the criminal action.

Thus, if the Constitution requires the same kind of adversary judicial proceeding to determine the existence of child pornography as it requires for obscenity, the statute here, interpreted in light of *McKinney*, provides one in

the criminal proceeding, which is the only proceeding in which the ISP can be subjected to any sanctions. Presumably, the Commonwealth then has the burden of proving that the offending site did display child pornography as defined at 18 Pa.C.S. § 6312. *See McKinney*, concurring opinion, Blackmun, J., 424 U.S. 677, 678. Before this full determination of a § 6312 violation, the ISP can ignore the Attorney General's notice, and the site will remain available to all. No government agent seizes the site or the ISP or anything in the possession of the ISP. The notice to the ISP does not even threaten prosecution.

Plaintiffs argue that the Constitution requires a whole host of participants in the adversary hearings - site owners, pornographers, Internet users everywhere. Plaintiffs' Memorandum, pp. 49-51. No case has imposed such a requirement. In the obscenity cases Plaintiffs cite, the party for which the Court required a pre-seizure hearing was the retailer. General procedural due process concepts would not require such large scale proceedings. *Mathews v. Eldridge*, 424 U.S. 319, 335 (1976). The interests in maintaining the alleged child pornography on the Internet are weak, the governmental interests in suppressing it are strong, the expanded proceedings would be unwieldy, and the additional participants would not make the determination of child pornography more accurate.

B. An *ex parte* judicial hearing constitutionally suffices to determine whether a web site is child pornography, and a finding of probable cause of child pornography is effectively a finding of child pornography.

Even if the Court considers only the statutorily required proceedings held before the common pleas court issues its initial order of authorization, the proceedings meet First Amendment and Due Process requirements because the relevant determination is child pornography, not obscenity. Government has powerfully compelling interests in suppressing child pornography, child pornography has no claim to First Amendment protection, and child pornography is easy to identify.

1. The compelling interests against, the lack of interests supporting, and the straightforward definition of child pornography make an adversary hearing before its suppression constitutionally unnecessary.

The cases upon which Plaintiffs rely all deal with obscenity. They require an adversary judicial proceeding because, where the issue is obscenity, such a proceeding reduces the risk that protected speech will be suppressed. Suppression of obscenity has inherent risks because the suppression is based entirely on the materials' communicative effects, and the First Amendment generally protects communicative effects. Furthermore, with obscenity, the line between the protected and unprotected depends on difficult-to-discern evaluative factors, and material close to the line may still have high protection. *See Fort Wayne Books, Inc. v. Indiana,* 489 U.S. 46 (1989); *Blount v. Rizzi,* 400 U.S. 410 (1971); *Freedman v. Maryland,* 380 U.S. 51 (1965); *Kingsley Books v. Brown,* 354 U.S. 436 (1957). Thus, the cases consistently note that

constitutionally protected expression "is often separated from obscenity only by a dim and uncertain line." *Blount v. Rizzi,* 400 U.S. at 416, 417; *Quantity of Copies of Books v. Kansas,* 378 U.S. 205, 210 (1964); *Bantam Books, Inc. v. Sullivan,* 372 U.S. 58, 65, 66 (1963).

The test for obscenity has always been difficult to discern and apply. Still today, it requires weighing of several nebulous factors. Under the current test, unprotected obscene material is only that which depicts sexual conduct in a "patently offensive way;" "taken as a whole, appeals to the prurient interest" of the average person applying contemporary community standards; and, "taken as a whole, lacks serious literary, artistic, political, or scientific value." *Miller v. California,* 413 U.S. 15, 24 (1974). These standards require sophisticated evaluation aided by competing viewpoints. The need for accuracy, and, thus, for procedural protections, is particularly acute where government seeks pre-publication (or pre-performance) suppression or censorship, because no one can fully know the speech until it is actually made. *Southeastern Promotions Ltd v. Conrad,* 420 U.S. 546, 558, 559 (1975).

Child pornography visible on the Internet is quite different from possibly obscene books or films. At the outset, it is not awaiting publication or performance. It is already there. Anyone can see it. No adversary judicial proceeding is needed to determine what can be seen on an ISP's services.

More importantly, the stronger government interests in suppression of child pornography weigh in favor of less rigorous pre-

suppression procedures. Government may suppress child pornography not just because it offends some people or reduces public morality, but because it is a critical element in the sexual exploitation and sexual abuse of the children who are displayed in it. *New York v. Ferber,* 458 U.S. at 757-762. They are abused in the performance, and they are abused in the permanent record made of their degradation. Child pornography also is used to seduce more children into sexual activity. For these reasons, government has powerfully compelling interests in suppressing it at every step of its production, distribution, and use. *New York v. Ferber*, 458 U.S. at 757, 759, 764; *Osborne v. Ohio,* 394 U.S. 103, 110, 111 (1990).[8]

The Supreme Court emphasized the difference between child pornography and mere obscenity when it held that government may constitutionally outlaw private possession of child pornography whereas it may not outlaw private possession of merely obscene material. *Compare Osborne v. Ohio,* 495 U.S. 103 (1990) to *Stanley v. Georgia,* 394 U.S. 557 (1969). The Court said, "the interests underlying child pornography prohibitions far exceed the interests justifying the Georgia law at issue in *Stanley*." 495 U.S. at 108. In the same way, the interests supporting suppression of child pornography justify occasional suppression of some material that is close to, but not quite, child pornography.

---

[8] Indeed, the Pennsylvania statute defining child pornography, and incorporated into the Internet Child Pornography statute at issue here, is titled, "Sexual abuse of children." 18 Pa.C.S. § 6312.

The Fourth Circuit has underscored "the fundamental distinction between child pornography and adult pornography." *U.S. v. Matthews,* 209 F.3d 338, 345 (4th Cir. 2000). "The government's interest in prohibiting the distribution of adult pornography — to protect 'the sensibilities of unwilling recipients,' ... pales in comparison to its interest in prohibiting the dissemination of child pornography — to prevent 'sexual exploitation and abuse of children.' " *Id.* The court there held that a journalist could not defend federal transmission of child pornography charges on the ground that he was creating a work of journalism.

In addition, child pornography's absence of First Amendment protection, and the weak protection of anything close to it, weigh against the need for an adversary judicial process when considering child pornography. The Supreme Court accurately said, "We consider it unlikely that visual depictions of children performing sexual acts or lewdly exhibiting their genitals would often constitute an important and necessary part of a literary performance or scientific or educational work." *New York v. Ferber,* 458 U.S. at 762, 763, 764. Even works that as a whole contain serious literary, artistic, political, or scientific value may contain child pornography that the government may outlaw. 458 U.S. at 761. The First Amendment can accept occasional suppression of material that is so close to child pornography that a judge mistakes it for child pornography.

Perhaps even more importantly, both the constitutional test and Pennsylvania's law defining child pornography can be applied accurately without an adversary judicial proceeding because the tests do not include the fluid, vague, evaluative elements of the obscenity test. For the same reason, a finding of *probable cause* that visual material is child pornography effectively equals a finding that the material *is* child pornography. That is, under the child pornography legal standards, visual material either clearly is or clearly is not.

Constitutionally, government may suppress child pornography without a showing that, taken as a whole, it appeals to the prurient interest of the average person. Government may suppress child pornography even if its depictions of sexual conduct are not "patently offensive." Government may suppress child pornography even if it is part of a work that, taken on the whole contains serious literary, artistic, political, or scientific value. *New York v. Ferber*, 458 U.S. at 761, 764.

Under the unquestionably constitutional Pennsylvania law, pictures are child pornography if they show a child under the age of 18 years engaging in or simulating any of the following:

> sexual intercourse as defined in section 3101 (relating to definitions), masturbation, sadism, masochism, bestiality, fellatio, cunnilingus, lewd exhibition of the genitals or nudity if such nudity is depicted for the purpose of sexual stimulation or gratification of any person who might view such depiction.

18 Pa.C.S. § 6312(a).[9] The test is based literally on what the viewer sees and is stated in objective, error-proof terms. Material clearly violates § 6312 or it does not. The decision does not require a laborious, fuzzy, evaluative determination. No factors need be weighed.[10] While § 6312 does have some exceptions, they too are objective, clear, and determinable on sight: the section does not apply to material that is "brought or caused to be brought into this Commonwealth, or presented for a bonafide educational, scientific, governmental or judicial purpose." § 6312(f). The standards are particularly easy to apply to Internet material, where pictures are generally accompanied by graphics that hype their purpose.

Pure Fourteenth Amendment procedural due process philosophy leads to the same conclusions. Procedural due process promotes a reasonably accurate decision when government seeks to deprive a person of constitutionally protected interests. *Goss v. Lopez*, 419 U.S. 565, 579, 580 (1975); *Morrissey v. Brewer*, 408 U.S. 471, 479, 480, 484 (1972). It is a flexible concept, and the degree, and timing, of process is generally determined by weighing three factors:

---

[9] Sexual intercourse is defined at 18 Pa.C.S. § 3101 as "its ordinary meaning" and "intercourse per os or per anus, with some penetration however slight; emission is not required."

[10] The Pennsylvania courts have upheld the statute against a vagueness challenge. *Commonwealth v. Savich,* 716 A.2d 1251 (Pa.Super.1998) *appeal denied* 738 A.2d 457, 558 Pa. 640 (1999). Of course, the U.S. Supreme Court in *Ferber* upheld the similar New York statute there against an overbroadness challenge.

> First, the private interest that will be affected by the official action; second the risk of an erroneous deprivation of such interest through the procedures used, and the probable value, if any, of additional or substitute procedural safeguards; and finally, the Government's interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirements will entail.

Mathews v. Eldridge, 424 U.S. 319, 335 (1976). Where no facts are, or can be, in dispute, procedural due process does not even require an opportunity to be heard. *Connecticut Dept. of Public Safety v. Doe,* 123 S.Ct. 1160, 1164 (2003); *Codd v. Velger*, 429 U.S. 624 (1977). Here, no one has any constitutionally protected interests in child pornography, and no one has significant interests in anything close to it. The government has strong interests in suppressing child pornography as extensively and as promptly as possible. Review by a judge alone poses little risk of erroneous decision. A judge can easily and unerringly decide whether depictions meet the statutory definition of child pornography. If any risk of error remains at all, an adversary proceeding will not reduce it appreciably. No one interested in defending the material would likely appear.

2. Decided federal cases have held that an adversary hearing is not required before suppression or seizure of child pornography.

A number of cases have applied both the First and Fourteenth Amendment thinking described above, most recently, the Court of Appeals for the Tenth Circuit in *Camfield v. City of Oklahoma City,* 248 F.3d 1214, 1224-

1228 (10th Cir. 2001). There, the court reviewed the qualified immunity of several Oklahoma City police officers who had seized copies of the film *The Tin Drum* because they believed it contained child pornography as defined by Oklahoma law. Before the police seized the film, they had obtained an informal and *ex parte* opinion of a local judge that the film did contain scenes that were child pornography. The plaintiff claimed that the seizure was invalid because it was not preceded by the procedural steps specified in the obscenity cases like *Fort Wayne Books*.

Applying qualified immunity analysis, the *Camfield* court first considered whether the police officers had violated the Constitution at all. The court rejected the idea that the obscenity case procedures apply when government seeks to remove child pornography from public access, for two reasons: (1) child pornography has less claim to constitutional protection than obscenity, and (2) child pornography is not as difficult to determine as obscenity. 248 F.3d at 1227. The court then decided that because the Oklahoma law included an exception for bona fide works of art that do not appeal to the prurient interest, it had incorporated part of the evaluative obscenity test, and a pre-seizure adversary judicial hearing was still required. But it said that, other than that exception, "an OCPD officer could reasonably have made the factual determination of whether certain scenes in *The Tin Drum* satisfied the definition of child pornography in" the Oklahoma statute (which was similar to 18 Pa.C.S. § 6312). 248 F.3d at 1228.

The court in *Camfield* cited, appropriately, a number of cases upholding the sufficiency of search warrants for child pornography. These cases hold that such warrants, and applications for them, need not describe the items to be seized in as much detail as warrants for obscene materials because law enforcement officers can easily determine what is or is not child pornography, stated in those simple terms or in the language of statutes like 18 Pa.C.S. § 6312. *United States v. Simpson,* 152 F.3d 1241, 1247 (10th Cir. 1998) ("the words 'child pornography' need no expert training or experience to clarify their meaning"); *U.S. v. Kimbrough,* 69 F.3d 723, 727, 728 (5th Cir. 1995) ("Identification of visual depictions of minors engaging in sexually explicit conduct, in comparison [to determination of obscenity], is a factual determination that leaves little latitude to the officers"); *U.S. v. Koelling,* 992 F.2d 817, 821, 822 (8th Cir. 1993) ("Most minors look like minors and most adults look like adults, and most of the time most law enforcement officers can tell the difference. The Constitution requires no greater precision."); *U.S. v. Hurt,* 808 F.2d 707, 708 (9th Cir. 1987) ("Any rational adult person can recognize sexually explicit conduct engaged in by children under the age of 16 when he sees it").

The *Camfield* court then cited to a district court that also had noted the relevance of the child pornography search warrant cases to the need for pre-enforcement adversary hearings. That district court had said that these "child pornography holdings demonstrate that courts do not require more

rigorous procedural safeguards or an adversarial hearing prior to seizure when law enforcement officers have objective and non-evaluative criteria by which to make their determinations." *Boggs v. Merletti,* 987 F.Supp. 1, 8 (D.D.C. 1997).

Relying on the same concepts, the Seventh Circuit, in *United States v. Moore,* 215 F.3d 681 (7th Cir. 2000), held that a person could be arrested for possession of child pornography without a judicial warrant, even though *Roaden v. Kentucky,* 413 U.S. 496 (1973) requires a warrant before seizure of allegedly obscene films incident to an arrest. The Seventh Circuit distinguished between obscenity and child pornography, stating first, "the concern with chilling protected speech by regulating arguably obscene material, which is presumptively protected under *Roaden* ... is outweighed by the compelling state interests in protecting children in the case of child pornography." 215 F.3d at 686. The court continued, "[t]he 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.*

Similarly, the District of Columbia Circuit found that publication policies of various producers of books, magazines, and films could not be "chilled" by provisions of a federal law authorizing forfeiture of child pornography. *American Library Association v. Barr,* 956 F.2d 1178, 1192 (D.C. Cir. 1992). The publishers claimed that they were uncertain what the law covered. The court responded that child pornography is not uncertain.

"However hazy the line between obscenity and protected speech, the line between eighteen years old and under is not 'dim and uncertain' " 956 F.2d at 1192. Moreover, the types of sexually explicit conduct statutorily defining child pornography, "would be readily apparent to anyone." *Id.* The types of conduct described there (18 U.S.C. § 2256(2)) were similar to those found at 18 Pa.C.S. § 6312(a): sexual intercourse, bestiality, masturbation, sadistic or masochistic abuse, and lascivious exhibition of the genitals. 956 F.2d at 1181.

3. The Constitution does not require an adversary hearing or a standard greater than probable cause before issuance of the initial court order and the notice of court order to an ISP under the statute here (18 Pa.C.S. §§ 7627, 7628).

Thus, the statutory procedures that apply here before issuance of the initial order of authorization by themselves comply with the Constitution. Under the statute, a judge reviews a web site before issuing the order (which authorizes the Attorney General to notify an ISP to remove or disable access to the site). A judge, of course, is an independent decision-maker who can reject the request, ask for additional information, or request participation by other parties. Indeed, the Statute expressly states that the judge may require, "additional testimony or documentary evidence." 18 Pa.C.S. § 7626(9). However, just by looking at the site, without an adversary proceeding, a judge can, to a constitutionally acceptable degree of accuracy, determine whether or not it is child pornography, as defined at 18 Pa.C.S. § 6312(a). Although the statute authorizes an order based on probable cause, the clarity of the child

pornography definition makes probable cause identical to a full finding. The display is either child pornography under the law or it is not.

Plaintiffs raise a question about virtual child pornography. This is material created completely by computer rendering that depicts children but uses no real children. Because it uses no real children, its legality must be measured under obscenity standards, not laws like 18 Pa.C.S. § 6312. *Ashcroft v. Free Speech Coalition*, 122 S.Ct. 1389 (2002). Presumably, true virtual material could not be a child pornography item under 18 Pa.C.S. § 7622 or the subject of a court order under § 7627, and a judge would have to distinguish it from pictures using real children in whole or in part. However, completely virtual material should not be difficult to detect, if it exists.

V. INFORMAL NOTICES DO NOT VIOLATE THE FIRST AMENDMENT BECAUSE THEY TOO ARE ISSUED AFTER DETERMINATIONS OF CHILD PORNOGRAPHY MADE WITH CONSTITUTIONALLY SUFFICIENT ACCURACY AND ALSO BECAUSE THEY ARE INFORMAL AND NON-COERCIVE.

Plaintiffs claim that Defendant's issuance of informal notices to ISPs rather than only notices of court orders violates the First and Fourteenth Amendments for the same reason that they challenge the statute itself. Relying particularly on *Bantam Books, Inc v. Sullivan,* 372 U.S. 58 (1963), as well as cases like *Blount v. Rizzi,* 400 U.S. 410 (1971) and *Freedman v. Maryland,* 380 U.S. 51 (1965), they again claim that any suggestion that the ISP should disable access to a child pornography web site must be preceded by an adversary judicial proceeding. However, for the same reasons that a judge proceeding *ex parte* can constitutionally determine child pornography, a law enforcement officer can make the determination with constitutionally sufficient accuracy. Furthermore, the informal notices are not coercive. Failure to comply with them incurs no sanction at all.

A. Law enforcement officers can determine child pornography with constitutionally sufficient accuracy.

Bantam Books also considered a case where the non-judicial determination was of obscenity (or less), not child pornography. There, a State Commission to Encourage Morality in Youth decided that certain books and magazines were objectionable for sale or display to youths under 18, notified the publishers' distributors of the finding, warned them that they were subject to criminal prosecution, and distributed the publication blacklist to local

police, who usually visited the distributors and asked what action they had taken. The Court held that even if the vague term "objectionable" meant obscene, the coercively applied finding could not be made without judicial superintendence. Child pornography was not part of the case. Similarly, in the other cases upon which Plaintiffs rely, obscenity, not child pornography, was the issue.

However, where child pornography was the question, the Tenth Circuit in *Camfield* stated that "an OCPD officer could reasonably have made the factual determination of whether certain scenes in *The Tin Drum* satisfied the definition of child pornography in" the Oklahoma statute. 248 F.3d at 1228. The Seventh Circuit in *Moore* stated that "application of child pornography standards ... is within the competency and experience of police officers." 215 F.3d at 686. The search warrant cases cited above all relied on the ability of law enforcement officers to identify child pornography when authorized to search for it. The compelling governmental interests in the suppression of child pornography and child pornography's absence of First Amendment protection likewise weigh in favor of a prompt, efficient process. These conclusions also follow from the *Mathews v. Eldridge* pure Fourteenth Amendment test: the private interests in child pornography-like material are weak, the government interests in suppressing child pornography are strong, and the risk of erroneous determination of child pornography by law enforcement officers is low.

Here, law enforcement officers employed by the Office of Attorney General determine that material they observe through an ISP's services is child pornography as defined at 18 Pa.C.S. § 6312 before sending the ISP an informal notice. Given the objective standards of § 6312 and the visual nature of the material, they can make this determination with constitutionally sufficient accuracy. The State's strong interests in the suppression of child pornography, and the weak private interest in child pornography-like material, support this procedure.

B. The informal notices are not coercive.

Even if law enforcement agents were not able accurately to determine child pornography, they could still engage in the informal process that the Attorney General's agents were using without violating the Constitution. The informal notices were only informal and carried no sanction, or even prosecution, for non-compliance.

The Court in *Bantam Books* stated clearly that law enforcement officers may, without first employing judicial machinery, engage in informal contacts with persons suspected of violating laws against obscenity in an effort to bring about compliance. 372 U.S. at 71, 72. The problem in *Bantam Book*s was that the State Commission was not a law enforcement agency charged with enforcing the obscenity laws and it was not just giving the distributors fair pre-enforcement advice. The Commission acted as a censorship board and

attempted to intimidate the distributors, through threats of criminal prosecution, into compliance with its beliefs.

Consistently, the Third Circuit has held that when a public official is sued for allegedly causing a third party to take adverse action against speech rights, the official is not responsible unless he coerces the third party to act through particularly virulent conduct. Influence, urging, critical remarks are not enough. *McLaughlin v. Watson,* 271 F.3d 566, 573 (3d Cir. 2001). The court noted that public officials have speech rights too and cannot be too readily held liable for their words. *Id.* at 574.

Here, Defendant's informal notices did not coerce the ISPs. Here, the Internet Child Pornography Law specifically gives the Attorney General the power to bring court actions, the power to send notices of court orders, and the power to prosecute for failure to comply with a notice of court order. 18 Pa.C.S. §§ 7625, 7626, 7628. The Attorney General's agents sent the informal notices as a means of informing the ISPs that the agents had found what they concluded was child pornography accessible through the ISPs' services. The notices gave the ISPs the opportunity to disable the access without facing notices of court orders that would have carried criminal penalties for non-compliance. Failure to comply with an informal notice carried no sanction. Failure to comply with an informal notice was not grounds for prosecution.

The language of the informal notice was not coercive. At first it told the ISP that it must disable access to the identified web site, but it stated no

consequence at all if the ISP did not. At the beginning of 2003, the "must" was changed to "should," and the notice added that failure to comply would only result in a non-criminal application for a court order of authorization to the Attorney General that, if issued, then would have led to a notice of court order to the ISP directing disablement.[11] The informal notice process respected the ISPs by offering them an opportunity voluntarily to disable access to illegal material without facing any statutory deadlines or sanctions. Failure to comply carried no sanctions at all. An ISP could not be criminally prosecuted for failure to comply.[12]

Plaintiffs point to a press release that the OAG issued September 17, 2002 when the Montgomery County court issued its order regarding the sites accessed through WorldCom. Plaintiffs' Memorandum, p. 57. Plaintiffs claim that the press release was "aggressive public intimidation." However, it was nothing more than a routine announcement of the result of a court proceeding, with a limited description of the proceeding (a copy is Exhibit 2 to Plaintiff's Motion for TRO). It neither made accusations against WorldCom nor embarrassed it in any way.

---

[11] A copy of this most recent notice is attached to Defendant's Answer to the Complaint and to this Brief.

[12] A lawyer employed by America Online did testify at deposition that at a November 22, 2002 meeting, William H. Ryan, Chief of the Attorney General's Criminal Law Division, stated that the informal notices had the same effect as court orders. Mr. Ryan denies making such a statement. Even if he made it, the informal notices were clearly not the same as court orders; failure, or even blatant refusal, to comply carried no sanction. The lawyer, being a lawyer, must have known that.

The informal notice process did not subject the Attorney General to the procedures required when government seizes, or similarly coercively suppresses, obscenity. The Court should allow it to continue.[13]

VI. THE STATUTE, AND INFORMAL NOTICES, AS APPLIED TO ISPs THROUGH WHOSE SERVICES CHILD PORNOGRAPHY IS ACCESSIBLE, DO NOT VIOLATE THE SUBSTANTIVE REQUIREMENTS OF THE FIRST AMENDMENT BECAUSE THEY DON'T SUBSTANTIALLY IMPEDE FIRST AMENDMENT PROTECTED ACTIVITY.

Again, Pennsylvania's Internet Child Pornography Law does not require disablement of access to any web site that has First Amendment protection. Nor did the informal notices. The statutory notices require, and the informal notices requested, disablement of access only to "child pornography items". 18 Pa.C.S. § 7622. The First Amendment does not protect child pornography. Disablement of access to it violates no one's First Amendment rights.

The court applications that the statute authorizes must identify the child pornography items by their Uniform Resource Locators because the URLs provide access to the child pornography items. 18 Pa.C.S. § 7626(4). The court orders and notices of them can only require disablement of access to those URLs. Likewise, the informal notices that Defendant's agents were sending asked that the ISPs disable access only to specific sites identified by

[13] If the Court believes that the informal notice should be re-worded, or have additional language, the Court could allow the informal process to continue in the future conditioned on compliance with the Court's instructions.

their URLs. Nothing in the law or the notices directs or requests disablement of access to any other sites or addresses or locators or identifiers.

Plaintiffs claim that despite the narrow and legitimate language of the statute and the Attorney General's informal notices, the law burdens First Amendment protected speech because, to disable access to child pornography items, ISPs must, due to current technology, disable access to other web sites that do not display child pornography. This claim requires both legal and factual analysis.

A. Because the speech restrictions about which Plaintiffs complain are content-neutral, the Court should apply the intermediate scrutiny test.

Although Defendant contends that the Pennsylvania law, as applied, passes any of the substantive First Amendment tests, the Court should not employ the "strict scrutiny" test. Strict scrutiny applies only when government imposes content-based burdens on protected speech. Then, the regulation passes First Amendment muster if it is necessary to serve a compelling governmental purpose and is narrowly tailored to achieve that purpose. *U.S. v. Playboy Entertainment Group, Inc.,* 529 U.S. 803, 813 (2000); *Boos v. Barry,* 485 U.S. 312, 321 (1988). Then, government may not intentionally suppress lawful speech as the means to suppress unlawful speech or to serve any other purpose unless the need is strong and the effect on legitimate speech narrow.

However, the statute here does not restrain speech based on its content. Child pornography is not speech. Defendant does not have to justify restraints

on child pornography. As against child pornography, the Court has nothing to consider under any test. The speech restrictive effects about which Plaintiffs complain are not content-based. If an ISP disables its customers' access to other sites when it disables their access to a child pornography site, the disablement of the other sites has nothing to do with their content. Indeed, neither the statute nor the informal notices intend that the ISPs disable access to these other sites at all. The effect that Plaintiffs allege is content-neutral. In a closer case, the Supreme Court held that a federal law was content neutral where it required cable television operators to reserve a certain number of channels for local broadcasters. *Turner Broadcasting Systems, Inc. v. FCC*, 512 U.S. 622 (1994). Those "must-carry" provisions did not discriminate based on content.

Where government restricts speech without reference to its content, the courts apply "intermediate scrutiny." Under this test, the restriction is valid if (1) it furthers a substantial governmental interest, and (2) it restricts no more than necessary to further the government's valid interest, that is, it leaves open ample alternative channels of communication. *Ward v. Rock Against Racism*, 491 U.S. 781 (1989) (New York City could control bands' sound at bandshell in Central Park); *Clark v. Community for Creative Non-Violence*, 468 U.S. 288, 294 (1984) (Government could prohibit homeless demonstrators from sleeping overnight on the D.C. Mall and in Lafayette Park even though sleeping overnight was part of the demonstration); *United States v. O'Brien*, 391 U.S.

367, 376, 377 (1968) (Burning a draft card can be made a criminal offense even though the act was done as a means of expressing opposition to the draft). This test does not require that the restriction be the least restrictive or the most effective means of achieving the government's purpose. *Ward*, 491 U.S. at 797, 798; *Clark*, 468 U.S. at 296, 297, 299; *Hill v. Colorado*, 530 U.S. 703, 726 (2000).

The Supreme Court applied the intermediate test to a situation not unlike that presented here when it upheld an ordinance prohibiting all posters, including campaign posters, on utility poles to protect community esthetics. *Members of the City Council of the City of Los Angeles v. Taxpayers for Vincent*, 466 U.S. 789, 803-812 (1984). The Court also applied the test in *Turner Broadcasting Systems, Inc. v. FCC, supra.* where the issue, similar to here, concerned restrictions on material carried by broadcast media. This Court should apply the "intermediate scrutiny" test in this case.

B. The statute and the informal notice process serve a compelling governmental purpose.

Government has a compelling interest in stopping child sexual abuse, wherever it occurs. *Ferber,* 458 U.S. at 756-58, 765, 766. Suppression of child pornography directly serves that interest. *Id.* at 759-762. Restricting child pornography's availability on the Internet substantially serves the interest. The Internet makes distribution of child pornography easy, safe, and profitable. The creators need only post a web site, which they can do from anywhere in the world. They can move their sites from place to place electronically. Using the

Internet, they can send their evil product anywhere. Consumers can receive the product over wires right in the comfort of their homes. They do not have to venture into risky neighborhoods, they run little risk of discovery, they can pay easily with credit cards. As a result of the Internet's easy distribution process, more and more children are sexually abused. Any interference with the distribution network reduces the abuse. *See U.S. v. Rodia,* 194 F.3d 465, 473-480 (3d Cir. 1999) (discussing the complex nature of child pornography distribution).

C. Neither the statute nor the informal notice process restrains an unconstitutionally excessive amount of legitimate speech.

Even under strict scrutiny, valid government regulation of speech can include collateral restriction of some speech that government has no interest in regulating. In *Ashcroft v. American Civil Liberties Union*, 122 S.Ct. 1700 (2002), the Court considered a portion of a federal law prohibiting persons from placing on the Internet "material that is harmful to minors." The material harmful to minors was defined in part by reference to "contemporary community standards." The Court upheld application of "contemporary community standards" even though standards differ from community to community and even though material posted on the Internet can be accessed in any community. Thus, an Internet publisher might be unable to publish material that is consistent with community standards some places (and so First Amendment protected there) because it is inconsistent with community standards in other places. An Internet user might be unable to access material

consistent with his community's standards because it is inconsistent with another community's standards.

Also, the Supreme Court has upheld forfeiture of a book seller's entire inventory based on convictions for transporting and selling only certain items of materials found to be obscene. *Alexander v. United States,* 509 U.S. 544 (1993). The government intentionally took materials never found or alleged to be obscene, and put the seller out of business.

Certainly, then, here, where neither the statute nor the informal notices intend any "collateral damage," where any collateral damage has nothing to do with speech content, and where the statute serves such an important purpose, the First Amendment can accept some restraint on some protected speech. The statute does not attempt or intend to suppress lawful speech or even possibly lawful speech. Under the applicable intermediate scrutiny test, unintended, content-neutral restriction on speech need not be the least restrictive means of meeting the government's purpose. It need only leave open ample alternative channels for speech.

Neither the statute, the statutory notices, nor the informal notices burden much protected speech.

The informal notices did not restrain any protected speech at all. They were not coercive. Failure to comply carried no sanction and did not subject the ISP to prosecution. Any disablement of access was the ISP's voluntary act

of cooperation, not an action of State actors. Moreover, the informal notices requested disablement only of child pornography sites.

Although a notice of court order issued under the statute can carry a criminal sanction for failure to comply (although the notice does not say so), it does not require an ISP to disable access to the identified site by any particular method. Nor did the informal notices. Nor does the technology. The ISPs have several methods readily available, and the method chosen was and is completely the decision of the ISPs, not State actors. Yet, the "overblocking" about which Plaintiffs complain has resulted from the method some ISPs chose to disable access. The ISPs had and have options for disabling access that would and will not block any, or as many, sites, as Plaintiffs claim were blocked in the past.

An ISP can disable its customers' access to a child pornography site quickly and easily by finding the host upon whose services the offending site is located and asking that host to remove it. *See* Complaint ¶¶ 87, 88; Memorandum in Support of Plaintiffs' Motion, pp. 37-39. This method has no effect on any other sites. Plaintiffs say that the government should contact the host, that this is a less restrictive alternative that the government should pursue. But asking the ISPs to do it restrains no First Amendment interests, and the ISPs, who are in the Internet business, can do it quickly and easily.

An ISP can disable its customers' access to a site by making an entry in its domain name servers that stops any requests for the full domain name, or

hostname, that identifies the site. This prevents requests for the child pornography site from reaching the site, but affects no other domain name. In that it affects no other domain names, it affects no or few other web sites.

With respect to entries in the domain name servers, Plaintiffs say two things. First, they say that the entries still may block access to innocent sites because innocent content may reside under the same domain name as child pornography content, in separate, independent sub-pages. However, once the Office of Attorney General staff became aware of this problem, they dealt with it in a manner that focused on the offensive content and protected the other content. When the OAG agents determined that child pornography resided as a page of an online community site, such as GeoCities.com or Terra.es, the OAG went directly to the site operator and asked it to remove the offending content. The OAG did not, in these cases, go to the ISP through which users accessed the Internet as a whole. This method, again, affected only the offending content. Defendant intends to continue this practice. Of course, an ISP that receives a notice (court or informal) to disable access to content residing on an online community can itself go to the operator of that community and request removal of the content. Other than the online community situation, innocent pages will not likely be found on sub-pages under a domain name used by child pornography.

Plaintiffs' second objection to the domain name server solution is that it is not completely effective. They say that a user can still get to the child

pornography site if he uses a domain name server other than one controlled by his ISP, or if he uses an "anonymizing proxy server," or if he switches ISP. This objection encompasses two arguments. First, Plaintiffs (or at least their expert) seem to say that because the users may have their computers assigned to domain name servers not controlled by the users' ISPs, the ISPs will be afraid to use the domain name server method (afraid of criminal liability for failure to disable access). They will instead block the sites' IP addresses, which risks substantial overblocking. Second, Plaintiffs seem to say that because the domain name server method (and even the IP address method) is not completely effective, its use, and the law, do not serve the governmental purpose of suppressing child pornography.

Neither the statutory nor the informal notices should "frighten" the ISPs out of the domain name server method. Neither the statute nor the notices of court orders it authorizes suggest any method for disabling access. The informal notices suggested no method. As between the domain name server and IP address methods, one would as easily expect an ISP to use the domain name server method because it reasonably effectively disables its customers' access to the objectionable site, and it least affects its customers' access to innocent sites. If the State courts ever consider the issue under today's technology, they will not impose criminal liability under the statute if an ISP uses the domain name server method, but some users evade it. The statute does not demand that access be disabled to any particular degree or with any

degree of permanency. The statute actually supports an interpretation lenient to the ISPs, in that it expressly does not require an ISP "to actively monitor its service or affirmatively seek evidence of illegal activity on its service." 18 Pa.C.S. § 7623. The ISP that uses the domain server method will be able to show the State court that it disabled access to the specified child pornography item using an accepted method and avoided a method that would probably have caused substantial collateral damage. The Pennsylvania courts, under Pennsylvania's Rules of Statutory Construction, would interpret the statute in a way that would support the ISP's reasonable actions. 1 Pa.C.S. §§ 1921, 1922, 1928.[14]

Throughout the administration of the statute, Defendant has accepted the domain name server method and the risks of evasion that it entails.[15] At the pre-effective date meetings between ISP and OAG representatives, OAG

---

[14] Section 1921 provides that legislative intent may be determined by considering several factors, including, "the consequences of a particular interpretation." Section 1922 requires presumptions that "the General Assembly does not intend a result that is absurd, impossible of execution or unreasonable," and that "the General Assembly does not intend to violate the Constitution of the United States or this Commonwealth." Section 1928 requires strict construction of penal provisions, that is, construction against imposition of penalties.

[15] Any argument that Pennsylvania district attorneys or future attorneys general might not be so reasonable constitutes a claim not ripe for consideration. *See American Library Assn. v. Barr*, 956 F.2d 1178, 1195-1199 (D.C. Cir. 1992). No district attorney has ever applied for a court order. No district attorney is likely to take positions significantly different from the Attorney General, who has developed extensive experience with the law. Indeed, before a district attorney can prosecute an ISP, the Attorney General must give the ISP notice of the court order, even if the order was obtained by a district attorney. 18 Pa.C.S. § 7628.

staff recommended it as a method. Verizon used the method substantially, and so informed the OAG agents in its responses to the informal notices, without objection. Later, when one ISP, EPIX, decided to use it exclusively, OAG staff did not object.

Defendant believes that the risks of evading domain name server filtering are not very high. Defendant's belief encompasses the risk that users will direct their computers to alternate domain name servers, the risk that they will use anonymizing proxy servers, and the risk that they will switch ISPs. Changing domain name servers requires technical savvy that most users do not possess, effort that most users do not want to expend, and risks that most users do not want to incur. Persons are unlikely to access child pornography from large corporate or organizational networks that do use their own domain name servers. People use the computers on these networks in their employment at times and in places where they will not want to have child pornography on their screens. Moreover, these organizations often filter, or at least monitor, their networks for illicit or non-employment related uses. Anonymizing proxy servers also require knowledge and skills that most users do not possess, and require effort, involve risks, and have operational downsides for the user. Using different ISPs also requires effort and expense. Also, the new ISP may be asked to disable access too.

Even if not complete, the domain name server filtering method still interferes with the distribution of child pornography and, thereby, its

production and the abuse of children inherent in the production. The method stops a number of people from reaching child pornography, for a time at least, reducing the number of people who might buy it, reducing the economic impetus to make it. Even if it doesn't completely stop everyone, it raises the cost of accessing child pornography, which discourages its accession, which discourages its production. At any rate, the alleged ineffectiveness doesn't increase burdens on First Amendment interests. Under intermediate scrutiny, at least, even a law that does impact speech does not have to be the most effective means of dealing with the problem government legitimately seeks to remedy. *Ward v. Rock Against Racism*, 491 U.S. at 797; *Clark v. Community for Creative Non-Violence*, 468 U.S. at 296, 297, 299.[16]

Technologically, ISPs could employ methods that focus even more specifically on the URL of the site than the domain name server method (and much more specifically than the IP address method) to filter out effectively requests only for that URL. However, these methods would, today, be an additional cost and operational challenge for many ISPs. Yet, some of the

[16] Recent commenters on the Internet and the Constitution have observed, "Nor should one assume that imperfections in Internet identification and filtering technology render these technologies useless. Regulation works by raising the cost of the proscribed activity, not necessarily by eliminating it. Computer-savvy users might always be able to circumvent identification technology, just as burglars can circumvent alarm systems. But they would do so at a certain cost, and this cost would be prohibitive for most." J.L. Goldsmith, A.O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 Yale Law Journal 785, 812, March 2001.

methods may be an option for smaller ISPs or those that have, or acquire, certain kinds of equipment.

And even IP address blocking can be used in those instances where a site is known, or likely, to be the only resident of the IP address.

The discussion of methods aside, and even assuming the statutory or informal notices coerce the disabling actions, and also force a method that blocks sites not identified in the notices, the effect on speech is still limited. A notice to an ISP goes only to that ISP. Any sites it might block remain accessible through other ISPs.

Plaintiffs argue that direct prosecution of those who create and post the child pornography items would be a less restrictive alternative that government could pursue in lieu of notices to ISPs through which the child pornography is accessible. This alternative, Plaintiffs claim, renders both the statute and the informal notices unconstitutional. However, a criminal prosecution, particularly limited to the producer, is not a very useful method of suppressing child pornography and the abuse of children inherent in it.

The First Amendment does not require that government regulate only through immediate criminal prosecution. Government may pursue civil proceedings to suppress obscene materials, at least as a preliminary step. *Kingsley Books v. Brown,* 354 U.S. 436, 441 (1957). It surely can pursue non-criminal procedures to suppress child pornography. More importantly, criminal prosecution of just the creators will not make a dent in child

pornography. Criminal prosecution is an expensive, difficult, and limited process under any circumstances, but creators of child pornography are particularly difficult quarry. The Supreme Court in *Ferber* stated, "there is no serious contention that the legislature was unjustified in believing that it is difficult, if not impossible, to halt the exploitation of children by pursuing only those who produce the photographs and movies" because production is a "low-profile, clandestine industry." 458 U.S. at 759, 760. The statement is even more true when the material is distributed over the Internet. The creators can be anywhere in the world and can hide behind the electronic complexities of the medium. After all, it is a *World Wide* Web.

Recognizing that direct prosecution of the creators is not a real alternative, Plaintiffs recommend that government ask web hosts to remove child pornography residing on their services. Plaintiffs say that this is an alternative means of suppressing child pornography on the Internet less restrictive than asking the ISPs to disable access to items that are only accessible through their services. But even if going to the host is a method, it probably will not be a fully successful method; it is not a complete alternative. Web site hosts can be anywhere in the world (again, it's a World Wide Web). They too can hide behind the complexity of the Internet's interconnected networks. Even if they can be found, and even if an American law enforcement officer or court can communicate with them, they have no reason to comply. So long as they have no people or assets in the regulating jurisdiction, no

sanctions can be enforced against them. Their child pornography will still be displayed through the ISPs providing Internet access service within the jurisdiction. Government still needs the authority to request, or demand, assistance from the ISPs through whose services child pornography is accessible. As the Court in *Osborne* said, government needs to stamp out child pornography "at all levels of the distribution chain" because much of the market "has been driven underground." 495 U.S. at 110. The Internet just makes the problem more difficult, and justifies even greater governmental effort.

The effectiveness of the statute in light of other alternatives today must also consider the future. Plaintiffs ask the Court for prospective relief: to declare the statute unconstitutional, effectively striking it from the books. The Constitution permits legislatures to legislate against harm before it has occurred, or before its has fully developed, or before the perfect remedy is technically available. *Turner Broadcasting Systems, Inc. v. FCC,* 520 U.S. at 212. The Internet is still a new and rapidly changing technology. *See Reno v. American Civil Liberties Union,* 521 U.S. 844, 849-593 (1997). Even today, technologically, ISPs could employ filtering methods at least as effective and more focused than either the domain name server method or the IP address method. These technologies, and probably others, will continue to be developed. As they are developed, the statute, starting from a more modest base, can be interpreted to accommodate them or even encourage them. This

situation differs from the inability of many sites to employ online user verification as described in *Reno v. American Civil Liberties Union*, 521 U.S. at 881, 882. There, nothing was available to every site that even worked to even a minimal degree. Here, the ISPs have a reasonable base from which to grow.

Indeed, the Third Circuit has looked to the future to find filtering a *less* restrictive alternative than direct sanctions against a producer of objectionable material. *American Civil Liberties Union v. Ashcroft,* 322 F.3d 240, 261-265 (3d Cir. 2003). In that case, the plaintiffs challenge a federal law that attempts to control Internet content by placing restraints on the producers of the material. The court held that government had alternatives less restrictive than restraints on the producers: government could encourage end users and the ISPs that deliver the content to block or filter out objectionable material. The court observed that the continual advances in technology make this alternative even more likely in the future. Applied here, the statutory and informal notices asking ISPs to disable access to objectionable material cannot be considered more restrictive than taking down the producer.

The Constitution should permit government to attack child pornography at all production, transportation, and distribution levels, particularly where the production, transportation, and distribution are on the Internet. The Constitution should permit government to go after the producers of child pornography, or direct ISPs to remove the producers from their networks, but should also permit government to ask ISPs to disable (block, filter out) access

to the child pornography that they deliver to their customers. Government has a compelling interest in the suppression of child pornography. The effects on First Amendment protected speech are small by comparison.

VII. THE STATUTE DOES NOT VIOLATE THE COMMERCE CLAUSE BECAUSE CHILD PORNOGRAPHY IS NOT COMMERCE AND BECAUSE THE LAW DOES NOT CAUSE ANY DISCRIMINATION AGAINST OR BURDEN ON LEGITIMATE COMMERCE.

Pennsylvania's Internet Child Pornography law does not violate the Commerce Clause either. Notices of court orders under the law may require ISPs to disable their customers' access to child pornography if it is accessible through their services in Pennsylvania. While their disabling actions may disable access of customers outside Pennsylvania, this effect does not interfere with interstate commerce. The Commerce Clause does not protect child pornography; child pornography is not commerce.

The Commerce Clause, U.S. Const. Art. I, Sec. 8 Cl. 3, provides a source of power for federal regulation of economic activity that substantially affects interstate commerce. *United States v. Lopez*, 514 U.S. 549 (1995); *McClain v. Real Estate Board of the City of New Orleans,* 444 U.S. 232 (1980). It also has a "negative" side that can limit state legislative powers. This state-limiting negative element primarily precludes state laws that discriminate against interstate commerce — laws that discriminate against out-of-state economic interests in favor of in-state interests, laws that attempt to implement local economic protectionism. *See West Lynn Creamery, Inc. v. Healy*, 512 U.S. 186, 192, 193 (1994); *Oregon Waste Systems v. Department of Environmental Quality*,

511 U.S. 93, 98, 99 (1994). The Supreme Court has also applied the negative Commerce Clause to strike state laws that directly control substantial quantities of wholly out-of-state economic transactions, particularly where the laws set prices, conflict with the laws of other states, and provide little local benefit. *See Healy v. Beer Institute*, 491 U.S. 324 (1989). However, the Court has long recognized that the states retain substantial power to regulate economic activity without offending the Commerce Clause, even though the regulated activity is part of or has an effect on interstate commerce. "Where the statute regulates even-handedly to effectuate a legitimate local public interest, and its effects on interstate commerce are only incidental, it will be upheld unless the burden imposed on such commerce is clearly excessive in relation to the putative local benefits." *Pike v. Bruce Church, Inc.*, 397 U.S. 137, 147 (1970); *Huron Portland Cement Co. v. City of Detroit*, 362 U.S. 440, 448 (1960).

If the State law does not impact commerce, it cannot be reviewed under the negative Commerce Clause at all. It is valid. The Supreme Court has long held that contaminated items, items unfit for consumption, items that spread disease and pestilence are not commerce, even if they move from state to state and even if they are sold from state to state. The Commerce Clause does not protect them or transactions in them. *Sligh v. Kirkwood,* 237 U.S. 52 (1915); *see also City of Philadelphia v. New Jersey,* 437 U.S. 617, 622 (1978); *Pike v. Bruce Church, Inc.,* 397 U.S. 137, 143, 144 (1970).

Surely, child pornography cannot be legitimate commerce. It is contaminated, noxious, unfit for consumption. It abuses children and causes abuse of children. Indeed, federal law, based on the Commerce Clause, makes its distribution in interstate commerce, including distribution by computer, a crime throughout the nation. 18 U.S.C. §§ 2252, 2252A. *See U.S. v. Rodia,* 194 F.3d 465 (3d Cir. 1999) (federal child pornography law was validly enacted pursuant to the Commerce Clause). It is likewise illegal under the laws of every State. *See* attached appendix of State laws. And Plaintiffs allege that "child pornography is illegal in all or almost all countries of the world." Complaint ¶ 86. It has no First Amendment protection, it can have no Commerce Clause protection.

Pennsylvania's statute requires disablement of access only to child pornography. Pennsylvania's statute and the federal law define child pornography similarly. 18 Pa.C.S. § 6312; 18 U.S.C. §2256(1), (2). As discussed above, the web sites to which ISPs must disable access will be child pornography. Even if the court orders (or informal notices) have extra-territorial effect, they do not offend the Commerce Clause.

Plaintiffs argue that, due to the Internet's current technology, the Pennsylvania law causes unintended disablement of access to sites that no one contends are child pornography. They argue that this effect runs throughout the nation and prevents legitimate, out-of-state transactions in violation of the Commerce Clause. However, this is a duplication of their First Amendment

argument. Defendant incorporates by reference the preceding argument in response to it - the law does not significantly cause suppression of legitimate Internet content anywhere.

Whatever out-of-state effect the statutory, or informal, notices might have on legitimate commerce does not discriminate against interstate commerce in favor of internal Pennsylvania commerce. The notices also do not control wholly out-of-state transactions in a way that will likely conflict with laws of other states. Arguably, because the Internet is an inter-connected network of networks, no transaction on it happens wholly outside any state where the Internet can be accessed. At any rate, even if other states adopt laws similar to Pennsylvania's statute, the laws will not conflict. The states' notices might create cumulative and overlapping burdens on ISPs, asking them to disable access to the same sites or additional sites. But the notices will not conflict with each other.

Cumulative adverse impact on transactions in other states does not by itself invalidate a state law. For example, in *CTS Corp. v. Dynamics Corp. of America*, 481 U.S. 69, 87-94 (1987), the Court upheld a state corporation law used by a corporation organized under it to block a nationwide tender offer for the corporation's shares, which were held throughout the nation. The law surely controlled out-of-state transactions and burdened interstate transactions, but could not conflict with other corporation laws because the corporation could only be incorporated in one state. By contrast, the price

affirmation law at issue in *Healy v. Beer Institute*, 491 U.S. 324 (1989) did pose probable interstate pricing conflicts to the point of "price gridlock." While some lower courts have stricken state Internet regulations because they have extra-territorial effects (*see* Plaintiffs' Memorandum. pp. 58-60), these decisions are not consistent with the Supreme Court's analyses in cases like *CTS Corp.* These lower courts have given excessive and unjustified deference to the novelty of the Internet. *See* J.L. Goldsmith, A.O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 Yale Law Journal 785, 827, 28, March 2001.

Finally, the statute's burdens on legitimate interstate commerce do not clearly exceed its benefits. In the Third Circuit, a law cannot be questioned under this balancing test unless it discriminates against interstate commerce, which the law here does not do. *Ford Motor Co. v. Insurance Commissioner*, 874 F.2d 926, 942-945 (3d Cir. 1989); *Instructional Systems, Inc. v. Computer Curriculum Corp.*, 35 F.3d 813, 826, 827 (3d Cir. 1994). Even aside from that requirement, a state law cannot be questioned just because it imposes burdens on interstate business, imposes regulation different from other states, increases costs, reduces consumer options, even prevents interstate transactions. *Id.; A.S. Goldmen & Co. v. New Jersey Bureau of Securities*, 163 F.3d 780 (3d Cir. 1999); *Tolchin v. Supreme Court of New Jersey*, 111 F.3d 1099, 1106-1110 (3d Cir. 1997)*; Aldens, Inc. v. Packel*, 524 F.2d 38, 47, 48 (3d Cir. 1975). Nothing about the Internet makes it immune from state regulation, any more than the national markets discussed in the cases: securities,

insurance, finance, corporate acquisitions. Neither statutory nor informal notices have the severe effects on interstate commerce that call the statute, or the informal notice process, into question.[17]

CONCLUSION

The Court should deny Plaintiffs' Motion for Declaratory Relief and for Preliminary and Permanent Injunctive Relief. The Court should vacate the Preliminary Injunction entered September 9, 2003, and should enter judgment in favor of Defendant.

GERALD J. PAPPERT
ACTING ATTORNEY GENERAL

BY: s/ John O. J. Shellenberger
John O.J. Shellenberger
Chief Deputy Attorney General
Identification No. 09714

OFFICE OF ATTORNEY GENERAL
21 S. 12th Street, 3rd Floor
Philadelphia, PA 19107-3603
Telephone: (215) 560-2940
Fax: (215) 560-1031

[17] Plaintiffs cite a federal statute at 47 U.S.C. § 230 that provides that ISPs shall not be treated as publishers or speakers of information provided by another "information content provider." This reference seems irrelevant, as Plaintiffs do not make a preemption claim. However, Pennsylvania's law does not attempt to treat ISPs as publishers or speakers of content, terms that appear to relate to defamation law. The Pennsylvania statute treats ISPs on its own terms, under its own terms.

APPENDIX OF STATE LAWS

Alabama	Ala. Code § 13A-12-190 (definitions); §§ 13A-12-191, 13A-12-191 (prohibiting pornographic display of persons under age 17).
Alaska	Alaska Stat. § 11.41.455 (unlawful exploitation of a minor)
Arizona	Ariz. Rev. Stat. Ann. § 13-3551 (definitions) § 13-3553 (sexual exploitation of a minor)
Arkansas	Ark. Stat. Ann. § 5-27-302 (definitions)
California	Cal. Penal Code § 311.3 (sexual exploitation of child); § 311.4 (employment or use of minor to perform prohibited acts)
Colorado	Colo. Rev. Stat. § 18-6-403 (sexual exploitation of children)
Connecticut	Conn. Gen. Stat. Ann. § 53a-193 (definitions)
Delaware	Del. Code Ann. title 11, § 1103 (definitions)
Florida	Fla. Stat. Ann. § 827.071 (sexual performance by a child)
Georgia	Ga. Code § 16-12-100 (sexual exploitation of children)
Hawaii	Hawaii Rev. Stat. § 707-750 (promoting child abuse in the first degree)
Idaho	Idaho Code § 18-1507 (sexual exploitation of a child)
Illinois	Ill. Rev. Stat. ch. 5, § 11-20.1 (child pornography)
Indiana	Ind. Code Ann. § 35-42-4-4 (child exploitation) § 35-49-1-4 (“minor”)
Iowa	Iowa Code Ann. § 728.1 (definitions)
Kansas	Kan. Stat. Ann. § 21-3516 (sexual exploitation of a child)
Kentucky	Ky. Rev. Stat. Ann. § 531.300 (definitions)
Louisiana	La. Rev. Stat. Ann. title 14, § 81.1 (pornography involving juveniles)

APPENDIX OF STATE LAWS

Maine	Me. Rev. Stat. Ann. title 17, § 2921 (definitions)
Maryland	Md. Crim. Law. Code Ann. § 1-101(g) (definition of "minor"); § 11-101(d) (definition of "sexual conduct"); § 11-101(e) (definition of "sexual excitement") § 11-202(f)(providing that "sexual conduct" has same meaning as in § 11-101); § 11-207 (child pornography)
Massachusetts	Mass. Gen. Laws. Ann. ch. 272, § 29A (posing or exhibiting child in state of nudity or sexual conduct); § 29B (dissemination of visual material of child in state of nudity or sexual conduct); § 31 (definitions of "lascivious intent," "minor")
Michigan	Mich. Comp. Laws Ann. § 750-145c (definitions of "child", "erotic nudity")
Minnesota	Minn.Stat. § 617.246 (use of minors in sexual performance prohibited)
Mississippi	Miss. Code Ann. § 97-5-31 (definitions of "child" and "sexually explicit conduct"); § 97-5-33 (depicting child engaging in sexual conduct)
Missouri	Mo. Rev. Stat. § 568.060 (abuse of a child)
Montana	Mont. Code Ann. § 45-5-620 (definition of "sexual conduct"); § 45-5-625 (sexual abuse of children); § 41-3-102 (6)(definition of "child" or "youth")
Nebraska	Neb. Rev. Stat. § 28-1463-02 (definitions of "child," "erotic nudity," "sexually explicit conduct"); § 28-1463.03 (visual depiction of sexually explicit conduct)
Nevada	Nev. Rev. Stat. § 200.700 (definition of "sexual conduct"); § 200.730 (possession of visual presentation depicting sexual conduct of person under 16 years of age unlawful)
New Hampshire	N.H. Rev. Stat. Ann. § 649-A:2 (definitions of "child," "sexual activity")

APPENDIX OF STATE LAWS

New Jersey	N.J. Stat. Ann. § 2C:24-4 (definitions of "child," "prohibited sexual act")
New Mexico	N.M. Stat. Ann. § 30-6A-2 (definition of "prohibited sexual act"); § 30-6A-3 (sexual exploitation of children; defining "child" as person under 18 years of age)
New York	N.Y. Penal Law § 263.00 (definition of "sexual conduct")
North Carolina	N.C. Gen. Stat. § 14-190.13 (definitions of "minor," "sexual activity," "sexually explicit nudity")
North Dakota	N.D. Cent. Code § 12.1-27.2-01 (definition of "sexual conduct"); § 14-10-01 (minors defined)
Ohio	Ohio Rev. Code Ann. § 2907.323 (illegal use of a minor in nudity-oriented material or performance); § 1021.2 (minors- procuring for participation in pornography)
Oklahoma	Okla. Stat. § 1024.1 (definition of "child pornography")
Oregon	Or. Rev. Stat. Ann. § 163.665 (definitions of "child," "sexually explicit conduct")
Rhode Island	R.I. Gen. Laws § 11-9-1.1 (child nudity prohibited in publications)
South Carolina	S.C. Code Ann. § 16-15-375 (definitions of "minor," "sexually explicit nudity")
South Dakota	S.D. Codified Laws § 22-22-24. (sale of child pornography as felony); § 22-22-24.1 (definitions of "child" or "minor", "nudity," and "prohibited sexual act")
Tennessee	Tenn. Code Ann. § 39-17-1002 (definitions of "minor," "sexual activity")
Texas	Tex. Penal Code § 43.25 (sexual performance by a child)
Utah	Utah Code Ann. § 76-5a-2 (definitions of "child

APPENDIX OF STATE LAWS

	pornography," "minor," "sexually explicit conduct")
Vermont	Vt. Stat. Ann. title 13, § 2821(1) (definition of "child"); § 2822 (use of a child in a sexual performance); § 2824 (promoting a recording of sexual conduct); § 2827 (possession of child pornography)
Virginia	Va. Code Ann. § 18.2-374.1 (production, etc. of sexually explicit items involving children); § 18.2-390 (definitions of "juvenile," "nudity")
Washington	Wash. Rev. Code Ann. § 9.68A.011 (definitions of "sexually explicit conduct," "minor)
West Virginia	W. Va. Code § 61-8C-1 (definitions of "minor," "sexually explicit conduct")
Wisconsin	Wis. Stat. § 948.01 (definitions of "child," "sexually explicit conduct")
Wyoming	Wyo. Stat. § 6-4-303 (sexual exploitation of children, definitions)

COMMONWEALTH OF PENNSYLVANIA

OFFICE OF ATTORNEY GENERAL

CRIMINAL LAW DIVISION
BUREAU OF CRIMINAL INVESTIGATIONS
CHILD SEXUAL EXPLOITATION UNIT

RE: Complaint Number:

INFORMAL NOTICE OF CHILD PORNOGRAPHY

To: , an Internet Service Provider

This notice is provided to you to advise you that child pornography, as defined at Section 6312 of the Pennsylvania Crimes Code, 18 PaCS 6312, has been accessed through your service at uniform resource locator www.[redacted]

You should 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.

You should ensure that: 1) Access to uniform resource locator www.[redacted] be denied to your subscribers who subscribe to your service from an address located within the Commonwealth of Pennsylvania using Internet service provided by [ISP] ; and 2) that the Attorney General or his designated agent is notified in writing (either U.S. Mail, email, or facsimile) that you have complied with this Informal Notice within five business days of said compliance. Accompanying your compliance notification must be a screen shot of the web page accessed by the Uniform Resource Locator demonstrating that access has been denied.

Failure to comply with this Informal Notice will result in this Office proceeding under Subchapter C of Chapter 76 of the Pennsylvania Crimes Code, 18 Pa.C.S. 7621 et seq, relating to Internet Child Pornography, to seek a Court Order directing you to deny access to said Internet site.

[Name]
Special Agent

[Address]
[Phone]
[Fax]
[e-mail]

Exhibit A

CERTIFICATE OF SERVICE

I, John O. J. Shellenberger, hereby certify that the foregoing Defendant's Brief in Opposition to Plaintiffs' Motion for Declaratory Relief and Preliminary and Permanent Injunctive Relief has been filed electronically and is available for viewing and downloading from the Court's Electronic Case Filing (ECF) system. A true and correct copy of the foregoing Brief was provided on December 24, 2003 by e-mail and hand delivery to:

Stefan Presser, Esquire
American Civil Liberties Union
125 S. Ninth St., Suite 701
Philadelphia, PA 19107

and by overnight mail, postage prepaid, to:

John B. Morris, Jr., Esquire
Center for Democracy & Technology
1634 I Street, NW, Suite 1100
Washington, D.C. 20006

D. MICHAEL FISHER
ATTORNEY GENERAL

BY: s/ John O. J. Shellenberger
John O.J. Shellenberger
Chief Deputy Attorney General
Identification No. 09714

OFFICE OF ATTORNEY GENERAL
21 S. 12th Street, 3rd Floor
Philadelphia, PA 19107-3603
Telephone: (215) 560-2940
Fax: (215) 560-1031