CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Working for Civil Liberties on the Internet

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

THE PENNSYLVANIA ISP LIABILITY LAW: AN UNCONSTITUTIONAL PRIOR RESTRAINT AND A THREAT TO THE STABILITY OF THE INTERNET

Center for Democracy & Technology
February 2003

EXECUTIVE SUMMARY

In February 2002, the Pennsylvania legislature enacted a law that imposes potential liability on Internet Service Providers for child pornography available anywhere on the Internet, even if the ISPs are not hosting the offending content and have no relationship whatsoever with the publishers of the content.

The goal of the statute – the elimination of child pornography from the Internet – is laudable. However, the law raises serious due process and First Amendment questions, and requires technical intervention that poses serious risks for the health of the Internet infrastructure.

The Pennsylvania Law violates constitutional principles of due process for at least two reasons:

- The law does not require notice to *any* of the individuals or entities whose speech (or ability to receive speech) is curtailed by court orders, nor does it mandate that those individuals or entities be granted *any* opportunity to participate in legal proceedings taking place pursuant to the law.

- The law requires a court to determine only that there is *probable cause* that the content in question is child pornography, a standard far weaker than is constitutionally required in proceedings that affect the availability of speech.

The law also violates the First Amendment, for at least three reasons:

- The procedures mandated by the law do not meet First Amendment requirements for government action that affects speech. To make matters worse, the Pennsylvania Attorney General has undertaken to make *secret* demands under the new law, blocking hundreds of Internet websites with no public notice or hearing whatsoever. The approach taken by the Attorney General constitutes a classic unconstitutional prior restraint on speech.

- The orders issued by the Pennsylvania court (and Attorney General) result in the blocking of web sites that have *nothing whatsoever* to do with child pornography, simply because those web sites use web hosting services that share a single Internet IP address among multiple web sites. This blocking of fully lawful websites – often in *secret* – is a blatant violation of the First Amendment.

- Moreover, the effects of the Pennsylvania blocking orders are felt far beyond the confines of Pennsylvania, as the orders ultimately block access by Internet users all around the country. Under First Amendment and Commerce Clause jurisprudence, lawmakers in one state cannot impose their views and values on citizens of another state.

The practical effects of this law on Internet technology are equally significant. Compliance with the law will carry potentially significant technical risks for the ISPs' networks, and the Internet in general. The routers and routing tables that direct the flow of content on the Internet were not designed to handle the kind of blocking envisioned by the statute. If Pennsylvania's blocking orders continue, the stability of the ISPs routers and routing table will be threatened, risking broad service failures.

Moreover, the ISP Liability Law does nothing to protect children victimized in the making of child pornography, or to help to prosecute those responsible for making or distributing the material. The law merely shields Pennsylvanians from the objectionable material, while the abuse of children is allowed to go on elsewhere.

The Center for Democracy shares the belief that child pornography has no place in civilized society. Powerful laws are already in place to combat child pornography, and CDT endorses their full enforcement. The Pennsylvania ISP Liability Law, however, is not an appropriate or effective way to solve this difficult problem.

I. FACTUAL BACKGROUND

A. The Pennsylvania Statute

In February 2002, the Pennsylvania legislature enacted a statute[1] (referred to here as the "ISP Liability Law") imposing potential liability on Internet Service Providers (ISPs) for child pornography available on the Internet, even if the ISPs are not hosting the offending content and have no relationship whatsoever with the publishers of the content. Essentially, the law makes any ISP that does business in Pennsylvania potentially liable for content anywhere on the Internet.

The ISP Liability Law requires that, upon receiving a notice from the Pennsylvania Attorney General, an ISP must promptly block or disable Pennsylvanians' ability to access the specified content. Under the law, the state Attorney General or any county district attorney can apply to a local judge for an order declaring that (a) certain content on the Internet is probably child pornography, and (b) the content can be reached through the services of a specified ISP. The entire court proceeding can go forward on an *ex parte* basis[2] (i.e., with the participation of just the government), with no prior notice to the ISP or the web site owner required, and no post-hearing notice to the web site owner. Such a proceeding contrasts with typical court proceedings that require notice to parties and an opportunity for both sides to be heard.

Under the law, a judge does not make any final determination that the challenged content is child pornography; instead, the judge needs only to find that there is "probable cause evidence" of child pornography.[3] Based on this *ex parte* probable cause determination, the state Attorney General notifies the ISP in question. The ISP then has five days in which to block all access to the specified content, or else face criminal liability.[4] As stated in the law, the location of the challenged content is specified by its "Uniform Resource Locator" (or URL, such as http://www.cdt.org or http://www.attorneygeneral.gov).[5]

The ISP Liability Law defines "Internet Service Provider" very broadly: "A person who provides a service that enables users to access content, information, electronic

---

[1] Pa. Stat. Ann. Title 18, § 7330. Although the text is on Lexis.com, there does not appear to be a freely available online version of the statute as it appears in the Pennsylvania Code. The text of Pa. House Bill 1333, enacting § 7330, is at http://www2.legis.state.pa.us/WU01/LI/BI/BT/2001/0/HB1333P3184.pdf.

[2] Pa. Stat. Ann. Title 18, § 7330(f).

[3] Section 7330(f).

[4] Sections 7330(a) and (c).

[5] Section 7330(e)(4).

mail or other services offered over the Internet."[6] This definition would not only reach actual ISPs (such as AOL or Earthlink), but also any establishment that provides access to the Internet (such as, for example, a library, school, hotel or Starbucks).

Critically, the ISP Liability Law imposes potential criminal liability for content that is merely "accessible through" an ISP's or access provider's service. The law lacks any requirement that the ISP have any connection to or responsibility for the content (such as if the content were created by the ISP or one of the ISP's customers). Instead, the potential liability is created simply because – as with any Internet service provided by any ISP – someone in Pennsylvania can reach content located anywhere on the Internet.

Moreover, once an order has been entered requiring that an ISP block content at a specified Internet URL, neither the judge nor the Pennsylvania Attorney General is required to withdraw the order if the challenged content changes. Indeed, no entity is required even to check to see if content changes, and even if an ISP did check, the law makes no provision for rescinding the order. Thus, the Internet site (the URL) appears to be blocked in perpetuity, and the ISP's liability for content on that site apparently can never be extinguished.

B. The Attorney General's Actions

As limited as the procedures set out in the Pennsylvania ISP Liability Law are, the Pennsylvania Attorney General has decided to bypass even those procedures. Instead, the Attorney General has undertaken a concerted campaign of *secret and wholly unreviewed* blocking of Internet content. The Attorney General has issued *hundreds* of secret blocking orders to many ISPs that operate in Pennsylvania, almost all without any public notice or judicial review whatsoever.

Instead of seeking the statutorily specified judicial "probable cause" review, the Attorney General instead issues directly to ISPs what are called an "Informal Notice of Child Pornography." In those Notices, the Attorney General informs the ISP:

> You must remove or disable access to [a specified Internet URL address] 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.[7]

---

[6] Section 7330(j).

[7] Nine examples of such Notices – sent to a single ISP over a two-day period in July 2002 – are appended as attachments to a court order that is discussed further below. *See* Order Requiring an Internet Service Provider to Remove or Disable Access to Child Pornography, In the Matter of the

According to the Attorney General, in the first five months that the Pennsylvania ISP Liability Law was in effect (through mid-September 2002), his office had used this secret Notice procedure to "disable access to more than 200 sites" on the Internet.[8]

The Attorney General indicated that the ISPs to which he has sent hundreds of secret Notices to block Internet sites have acquiesced to those demands in "the vast majority of cases."[9] One ISP, however, apparently refused to go along with the Attorney General's secret Notice procedure. In a July 25, 2002, letter to the Attorney General's office, WorldCom, Inc. responded to nine secret Notices (demanding that access to nine web sites be blocked) by explaining:

> WorldCom does not have any relationship to any of the sites listed in your informal notices: we do not host any of these sites, nor do we have any other legal or physical control over any of these sites.[10]

WorldCom offered to work with the Attorney General's office if that office decided to seek a court order. In response, and apparently without any notice to WorldCom or the web sites involved, the Attorney General sought and obtained a "probable cause" court order requiring WorldCom to block access to the web sites in question (as specified by URLs given in the court order).[11] The Attorney General also issued a press release that effectively accused WorldCom of facilitating access to child pornography.[12]

Application of D. Michael Fisher, Attorney General of the Commonwealth of Pennsylvania for an Order Requiring an Internet Service Provider to Remove or Disable Access to Child Pornography, Case No. Misc. 689 Jul 02 (Sept. 17, 2002 Court of Common Pleas, Criminal Division, of Montgomery County, Pennsylvania) [hereafter "Court Order"].

[8] "Montgomery County Judge Orders WorldCom to Disable Access to Child Pornography Internet Sites; First Court Action Taken by Pennsylvania Attorney General Fisher Under New PA Law," Press Release Issued by the Pennsylvania Office of Attorney General, September 18, 2002 [hereafter "Attorney General's Press Release]. Curiously, although the web site of the Pennsylvania Attorney General, www.attorneygeneral.gov, includes hundreds of press releases, it does not contain this press release. The text of the press release is available through the Google web site at http://216.239.53.100/search?q=cache:bimAO0YrjC4C:biz.yahoo.com/prnews/020918/phw046_1.html.

[9] *See* Attorney General's Press Release.

[10] Letter from WorldCom to Pennsylvania Attorney General's Office, July 25, 2002, appended as an attachment to the Court Order referenced above.

[11] *See* Court Order.

[12] *See* Attorney General's Press Release.

C. The Technical Impact to Date of the Law and the AG's Actions

Aside from the procedural and constitutional concerns about the ISP Liability Law (as discussed more fully below), there are serious *technical* problems raised by the Attorney General's orders to block hundreds of specified Internet URLs. Most critically, the only effective method to block access to URLs has two major side effects – the blocking cannot be confined to Pennsylvania, and more critically, the blocking *also* blocks web sites (and Internet speech more generally) wholly unrelated to the challenged content in question.

1. Methods of Blocking Access to a URL

Given the architecture of the Internet and ISPs, an ISP can take only two approaches to comply with an order from a court (or the Attorney General) to block access to a specific URL. Only one of the two approaches would be effective.

The *ineffective* method for an ISP to block access to a URL is to make changes to the ISP's DNS (or "domain name system") table, which is the database used to translate a URL (like www.cdt.org) into a numeric Internet Protocol (or IP) address such as 206.112.85.61. A DNS table could be modified so that if a user requests access to a URL, the correct IP address is *not* returned (and thus the user's browser cannot reach the URL). The critical problem with this approach, however, is that many DNS tables are available all across the Internet, and many users do not use the DNS table offered by their own ISP. Thus, even if an ISP modified its DNS table to block access to a specific URL, many of the ISP's users would still be able to access the URL (and thus the ISP would face criminal penalties under the Pennsylvania ISP Liability Law).[13]

The only way that an ISP can *effectively* block access to a URL is to block access to the numeric Internet Protocol (or IP) address to which the URL translates. The common method to block access to an IP address is to "null route" the IP address. To "null route" an IP address, an ISP enters an "exception" into the "routing tables" used by the ISP's routers (the physical devices that direct all Internet traffic toward the proper destinations).[14] Thus, an ISP could enter an instruction into a routing

[13] In addition to this critical defect, making ISP-specific changes to a single DNS table would run directly counter to the entire DNS system on the Internet, which generally assumes that DNS changes will be promulgated and replicated throughout the Internet. If an ISP were to change its DNS table in response to a court order, it would have to ensure that the false DNS information did *not* promulgate into the global DNS system.

[14] "Null routing is a way of routing traffic to the null interface (i.e. discard the traffic) from a particular IP address, which is useful if the IP address is the source of a denial of service attack." "NISCC Technical Note 01/02: Protecting your computer network," Jan. 2002, available at http://www.uniras.gov.uk/l1/l2/l3/tech_reports/NISCCTechnicalNote01.htm.

table such that any requests for a specific IP address (such as 206.112.85.61) would fail.[15]

In the case of the only known Court Order under the Pennsylvania law, this "null routing" is exactly what the ISP was forced to do. As the ISP (WorldCom) explained to the Attorney General's office:

> [D]ue to WorldCom's network architecture, it is not technically-feasible for us to block access to a site on the Internet based on the URL of that site; rather, the only technically-feasible solution for WorldCom to block access to a site not on our network is by means of null routing the Internet Protocol number of the site in question.[16]

Thus, in order to block access to certain URLs specified in the Court Order, the ISP would need to block access to the IP addresses to which those URLs translated.

2. Critical Problems Caused by Blocking IP Addresses

There are, however, three huge technical concerns raised by the concept of blocking IP addresses: (1) the IP address blocking must extend over all (or a large portion) of an ISP's network, mostly *outside* of Pennsylvania, (2) the IP address blocking also blocks *wholly unrelated web sites* that happen to share the IP address of an offending site, and (3) the IP address blocking will ultimately threaten the stability of the ISP's network and of the Internet itself. These problems are discussed in turn below.

First, the blocking reaches far outside of Pennsylvania. Except for small ISPs that only do business in Pennsylvania (and thus whose networks are entirely in that state), the routing tables used by an ISP cover the ISP's entire network, or a large geographic portion of a worldwide network (such as are operated by WorldCom, AOL, etc.). ISPs' networks simply are not constructed with state boundaries in mind, and the economics of an ISP's business require that an ISP use its routers to cover as large an area as the routers can reliably and efficiently cover. For many large ISPs, the routing table used for Internet traffic to and from Pennsylvania is the same routing table used for all traffic nationwide. Thus, blocking an IP address in

---

[15] A variation on this method of "null routing" would be to redirect request for one IP address to a different IP address (one that then returns an error message). With the approach described in text, the router itself would return the routing error message, while with this variation the error message would originate with a server external to the router. Although these two approaches have different technical implications, for all purposes addressed in this paper, these two methods to "null route" an IP address are functionally the same.

[16] Letter from WorldCom to Pennsylvania Attorney General's Office, July 25, 2002, appended as an attachment to the Court Order referenced above.

response to a Pennsylvania order will block the IP address for users far outside of Pennsylvania.

Second, the blocking reaches completely independent and unchallenged content. Blocking an IP address (especially for small websites) will in many cases block content *wholly unrelated* to the URL originally targeted. That is because it is very common for unrelated web sites to *share IP addresses*. For example, CDT's web site, www.cdt.org, is accessible at IP address 206.112.85.61. But that IP address is *also* used by more than six other web sites, including:

> www.cfp2002.org
> www.ciec.org
> www.consumerprivacyguide.org
> www.internetpolicy.net
> www.naisproject.org

Thus, a hypothetical order to block the URL www.cdt.org would also block these and other web sites.[17]

The practice of using shared IP addresses is very common with ISPs that offer web hosting services, especially hosting for smaller companies or web sites that do not alone warrant their own dedicated web server. As one Internet authority explains:

> Name-based web hosting is a technique that can be used when providing virtual web hosting services. Each web site that is hosted on a single machine shares a single public IP address. All HTTP GET requests received by this web server are answered according to the domain name supplied by the requesting client, enabling the web server to differentiate between multiple virtual sites on the one IP address.[18]

Indeed, the sharing of IP address is *required* for any new service provider seeking to provide web hosting services.[19] Before the American Registry for Internet Numbers ("ARIN," which controls IP addresses for North America) will allocate

---

[17] As implemented in the Apache web server product, which is used by more than 50% of all web servers worldwide, the ability to share IP address is termed "Virtual Hosting." *See* "Name-based Virtual Host Support," available at http://httpd.apache.org/docs/vhosts/name-based.html.

[18] APNIC, "Virtual web hosting FAQ," available at http://www.apnic.net/info/faq/virtualwebfaq.html.

[19] For a detailed discussion of the technical development of IP address sharing capability, see a recent report of Benjamin Edelman of the Berkman Center for Internet & Society at the Harvard Law School, entitled "Web Sites Sharing IP Addresses: Prevalence and Significance," available at http://cyber.law.harvard.edu/people/edelman/ip-sharing/ [hereafter "Edelman Report"].

any IP addresses to a new web hosting company, the company must demonstrate that it shares IP addresses among web sites.[20]

A recently completely analysis by Benjamin Edelman of the Berkman Center for Internet & Society at the Harvard Law School establishes that IP sharing is *very* widespread across the Internet.[21] According to Edelman's analysis of over 20 million .COM, .NET, and .ORG web sites active in December 2002, *over 85%* of the sites shared an IP address with another site, and *over two-thirds* of the sites shared an IP address with at least *fifty* other web sites.[22] In many cases, web sites share an IP address with *thousands* of other sites. For example, according to the Edelman Report, IP address 216.136.232.176 is used by 73,811 different web sites, and 216.21.229.199 is used by 82,290 different web sites.

Thus, in some cases an IP address may be shared by literally *hundreds, thousands, or even tens of thousands* of different, wholly independent web sites. Any order by the Pennsylvania Attorney General to block any one of those web sites will block them all.

Moreover, in addition to the shared IP address problem that is inherent in many web hosting operations, at least some of the Pennsylvania Attorney General's URL blocking orders have targeted web sites that by definition include huge amounts of content *wholly unrelated* to the challenged content. For example, one of the URLs specified in the Court Order discussed above was:

> www.terra.es/personal8/jenout/[23]

Terra.es is operated by the leading ISP in Spain, and is one of the leading Spanish language Internet sites in the world. As of 2001, Terra.es ranked in the top fifty sites accessed from within the United States (and was the top foreign language site accessed from within the U.S.).[24] A key component of the Terra.es service is a personal web page service, in which (like similar offerings in the U.S. from AOL and Geocities) individuals can create and post their own web pages.

---

[20] "ARIN Instructions For Using Name-Based Virtual Webhosting," available at http://www.arin.net/announcements/archive/name_based_hosting.html. As discussed in the Edelman Report, the entities that control IP addresses outside of North America have similar requirements.

[21] *See* Edelman Report, discussed in footnote 19 above.

[22] *See* Edelman Report.

[23] Court Order, page 2.

[24] "Top 50 Rankings also Show Terra.es Makes Steady Climb," ComScore Networks, June 21, 2001, available at http://www.comscore.com/news/pr_greetingcardsites_062101.htm.

The URL that the Pennsylvania court ordered the ISP to block is one of *thousands and thousands* of personal web pages hosted by terra.es. Entering the terra.es IP address into an ISP's routing table, however, will block *the entire* terra.es web site. Thus, based on the content of a single web page among thousands, access to thousands of independent web sites will be blocked (and, as noted above, will be blocked for users far outside of Pennsylvania).

Thus, as a result of the hundreds of blocking orders issued by the Attorney General, it is almost certain that hundreds (if not thousands) of wholly independent web sites have also been blocked.

Third, IP address blocking threatens the stability of ISPs, and ultimately of the Internet. Routers and routing tables simply were not designed to handle hundreds or thousands of null routing exceptions. Although it does not appear that the Pennsylvania Attorney General's blocking orders have yet damaged any ISP's network, if the orders continue (and if other governments also start issuing their own censorship orders), the stability of ISPs' routers and routing tables will be threatened. Moreover, the very act of making changes to a routing table can itself have harmful consequences. The history of the Internet has seen a variety of cases where changes to a routing table caused major service outages. For example, in October 2002, "a routing table issue led to about 20 percent of the WorldCom IP customer base in the US having problems accessing the Net."[25] This is just one example of routing table related outages that have occurred on the Internet.[26] The risk of broad outages caused by routing table problems will only increase if Pennsylvania and other governments continue to issue URL or IP address blocking orders.

II. THE PENNSYLVANIA ISP LIABILITY LAW AND ITS IMPLEMENTATION ARE UNCONSTITUTIONAL, ILLEGAL, AND NOT ULTIMATELY EFFECTIVE IN STOPPING CHILD PORNOGRAPHY

Without question, the general goal of fighting child pornography is laudable – such content has no place whatsoever in a civilized society. As far as CDT is aware, every country in the world outlaws child pornography, and vigorous international

[25] "WorldCom customers hit by outage," The Age, Oct. 4, 2002, available at http://www.theage.com.au/articles/2002/10/04/1033538763017.html. There is no indication that the October 2002 WorldCom outage was a result of actions by the Pennsylvania Attorney General.

[26] *See, e.g.,* "Net Outage: The Oops Heard 'Round the World," Wired, Apr. 25, 1997, available at http://www.wired.com/news/technology/0,1282,3442,00.html; *see also* http://www.bgpexpert.com/ (discussing routing table related outages).

law enforcement efforts are aimed at combating it.[27] CDT certainly endorses the goal of fighting child pornography.

The Pennsylvania ISP Liability Law, however, is the wrong way to accomplish that laudable goal. The law as written raises significant legal and constitutional issues, and the Attorney General's secret implementation of the law raises additional constitutional concerns. Moreover, in the end, the ISP Liability Law represents a misguided use of law enforcement resources, one that may in fact *hinder* the prosecution of those who create and distribute child pornography.

A. The Pennsylvania Law Violates Constitutional Principles of Due Process.

Because of the extremely broad impact of the ISP Liability Law – blocking Internet access far outside of Pennsylvania and blocking web sites wholly unrelated to the challenged site – the law impinges on the rights of a broad array of actors (many, if not most, located outside of Pennsylvania). A proposed court order that requires an ISP to block a URL directly impacts on the legal rights of a number of different individuals or entities:

- the ISP that will be subject to a court order;
- the owner/operator of the challenged web site;
- the visitors/users of the challenged web site;[28]
- the owners/operators of unrelated web sites that share the IP address of the challenged web site; and
- the visitors/users of the unrelated web sites that share the IP address.

Yet under the Pennsylvania ISP Liability Law, *none* of these individuals or entities receives any notice of the legal proceeding or any opportunity to participate in the proceeding. As the U.S. Supreme Court has made clear, this kind of lack of notice and opportunity to be heard runs directly counter to the very foundation of constitutional due process:

> "The fundamental requisite of due process of law is the opportunity to be heard." The hearing must be "at a meaningful time and in a meaningful manner." In the present context these principles require

[27] For information on international efforts against child pornography, see, e.g., http://www.usdoj.gov/criminal/ceos/hamletre.pdf.

[28] The owner of a challenged web site does not have any "right" to operate a site with child pornography, and visitors to the site similarly do not have a "right" to access child pornography. But, until there is a final and constitutionally valid judicial determination that certain content is in fact unlawful child pornography, the web site owners and visitors do have rights that must be protected.

> that [an individual] have timely and adequate notice detailing the reasons for a proposed [government action], and an effective opportunity to defend by confronting any adverse witnesses and by presenting his own arguments and evidence orally.[29]

The unconstitutionality of these procedural defects are made even worse by the fact that the ISP Liability Law only requires a court determination that there is "probable cause" that certain content is child pornography. This type of determination is far weaker than would be required in an ordinary criminal child pornography proceeding. The Supreme Court has noted that – as the name suggests – probable cause determinations only deal with "probabilities."[30] "[O]nly the probability, and not a prima facie showing, of criminal activity is the standard of probable cause."[31]

Thus, under the Pennsylvania ISP Liability Law, the rights of Internet service providers, publishers, and listeners (including many far outside of Pennsylvania) are permanently adjudicated without notice, without opportunity for hearing, and without even a certain judicial determination that the challenged content is illegal in the first place. This law fails to even approach the constitutional minimum requirements for due process, and thus it violates the Fourteenth Amendment of the U.S. Constitution.

B. The Pennsylvania Law Violates the First Amendment.

Beyond the due process problems inherent in the ISP Liability Law, the law also violates the First Amendment, for two independent reasons.

First, the procedures established by the law are wholly inadequate under First Amendment jurisprudence. The law operates as a system of permanent "prior restraint" – the blocking of speech prior to any full, adversarial, and final adjudication of the legality of the speech. As the Supreme Court has repeatedly made clear, "[a]ny system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity."[32]

In the vast majority of cases, the courts have struck down as unconstitutional state censorship regimes like the Pennsylvania law. The Supreme Court has, however,

---

[29] Goldberg v. Kelly, 397 U.S. 254, 268 (1970) (citations omitted), available at http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=us&vol=397&invol=254.

[30] Brinegar v. United States, 338 U.S. 160, 175 (1949). According to the Court, "probable cause" requires "less than evidence which would justify . . . conviction" but "more than bare suspicion." *Id.* (citations omitted).

[31] Spinelli v. United States, 393 U.S. 410, 419 (1969).

[32] Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 70 (1963).

allowed in very narrow cases the entry of a prior restraint against *obscene* speech (a category of speech analogous to the child pornography addressed by the Pennsylvania law), but *only* with the strictest of procedural safeguards. The Supreme Court has made clear that any effort to impose a prior restraint even on allegedly illegal speech (like obscenity or child pornography) must follow certain "procedural safeguards designed to obviate the dangers of a censorship system":

1. the government must bear the full burden of proving that the content is illegal;
2. any restraint must be limited to "the shorted fixed period compatible with sound judicial resolution";
3. there must be adequate notice to those affected by the censorship; and
4. there must be a full adversarial hearing.[33]

The Pennsylvania ISP Liability Law fails on *all* of these points. As with due process requirements, the law does not even begin to approach the constitutional safeguards required under the First Amendment.

Second, and wholly independent of the procedural inadequacy of the ISP Liability Law under both the First and Fourteenth Amendments, the law also violates the First Amendment because of its direct and harmful impact on constitutionally protected expression.

Child pornography is not protected expression under the First Amendment. But, as explained above, the impact of the Pennsylvania ISP Liability Law is to block access to hundreds or even thousands of web sites that have *nothing* to do with child pornography, simply because those web sites use a web hosting service that shares a single Internet IP address among multiple web sites. Thus, even assuming that the Pennsylvania censorship orders only identified URLs with actual child pornography,[34] the *impact* of those censorship orders reach far beyond illegal child pornography.

Just last year – *in a case involving a child pornography statute* – the U.S. Supreme Court struck down a federal criminal law precisely because of its impact on *protected* expression.[35] The Supreme Court could not have been more clear:

---

[33] *See* Freedman v. Maryland, 380 U.S. 51 (1965).

[34] Because of Pennsylvania's secrecy and lack of adversarial proceeding, this assumption cannot be tested.

[35] *See* Ashcroft v. Free Speech Coalition, 535 U.S. ___ (2002), available at http://www.supremecourtus.gov/opinions/01pdf/00-795.pdf.

> The Government may not suppress lawful speech as the means to suppress unlawful speech.... "[T]he possible harm to society in permitting some unprotected speech to go unpunished is outweighed by the possibility that protected speech of others may be muted ...."[36]

This Supreme Court holding *precisely* applies to the Pennsylvania ISP Liability Law. To paraphrase the Supreme Court, although the "objective [of the law] is to prohibit illegal conduct, [the] restriction goes well beyond that interest by restricting the speech available to law-abiding adults."[37] Because of its impact on constitutionally protected speech and the ability of Internet users far beyond Pennsylvania to access such speech, the ISP Liability Law is unconstitutional under the First Amendment.

C. The Pennsylvania Attorney General's Secret Censorship Demands Represent a Classic Unconstitutional Prior Restraint.

As discussed above, the Pennsylvania ISP Liability Law violates, by its own terms, both the First and Fourteenth Amendments to the Constitution. But the Attorney General's system of secret unreviewed censorship orders presents additional blatant constitutional problems.

The secret censorship system of the Attorney General is remarkably similar to the government scheme struck down in the landmark 1963 Supreme Court decision in *Bantam Books v. Sullivan*.[38] In that case, a Rhode Island state commission advised distributors that certain books and materials were deemed "objectionable" by the commission without judicial review. The commission asked for the distributors' "cooperation" in removing the material, and advised them of the commission's duty to recommend prosecution. The Supreme Court held that this form of informal censorship was in violation of the First and Fourteenth Amendments.

The Pennsylvania Attorney General censorship system is *directly* parallel to that struck down forty years ago in *Bantam Books*. Indeed, the Attorney General himself calls his system an "informal" one.[39] As the Supreme Court wrote forty years ago, "the system of informal censorship disclosed by this record violates the

---

[36] Ashcroft, 535 U.S. at ___ (slip opinion at 17) (citation omitted).

[37] Ashcroft, 535 U.S. at ___ (slip opinion at 14-15).

[38] *See* Bantam Books v. Sullivan, 372 U.S. 58 (1963), available at http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=us&vol=372&invol=58.

[39] *See* Attorney General's Press Release, cited above.

[First and] Fourteenth Amendment[s]."[40] The Attorney General's "informal" actions are equally unconstitutional.

D. The Pennsylvania Law Conflicts with Federal Law.

Beyond the myriad constitutional defects with the ISP Liability Law and the Attorney General's censorship scheme, the law also squarely conflicts with Section 230 of the Telecommunications Act of 1996.[41] That provision of federal law (which under our system trumps any conflicting state law) makes clear that ISPs should *not* be held liable for content that is merely accessible *through* the ISP. Under the system established by Congress in 1996 (and upheld and enforced by numerous courts across the country), the legal responsibility for content on the Internet lies with the individuals or entities that publish the content on the Internet, and *not* with ISPs through whose networks the content can be accessed.

The Pennsylvania ISP Liability Law runs directly counter to the federal legal regime created in Section 230. Moreover, the federal law *expressly* preempts any conflicting state laws: "No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with [Section 230]."[42] That, however, is precisely what the ISP Liability Law attempts to do.

E. The Pennsylvania Law Reflects Misguided Legislating and Law Enforcement.

Beyond the constitutional and legal defects inherent in the ISP Liability Law and the Attorney General's actions, the underlying approach taken by the Pennsylvania legislature is misguided and may even be harmful to the prosecution of child pornographers.

That child pornography is abhorrent is without question. But as the Supreme Court made crystal clear in 2002, the paramount goal addressed by child pornography laws is the protection of the children who are abused during the production of the material.[43] Under the First Amendment, the Supreme Court has held, child pornography lacks any constitutional protection *not* because of content of the resulting images (which may or may not be "obscene"), but because of the

---

[40] Bantam Books, 372 U.S. at 71.

[41] *See* 47 U.S.C. § 230.

[42] 47 U.S.C. § 230(e)(3).

[43] *See* Ashcroft, 535 U.S. at ___ (slip opinion at 11-12).

overriding governmental interest in protecting the children who are victims of child pornographers.[44]

Yet the ISP Liability Law *does absolutely nothing* to help protect the children victimized in the making of child pornography, or to help prosecute those responsible for making or distributing child pornography. Effectively, the Pennsylvania legislature has said: (1) we recognize that children are being victimized in the creation of child pornography, but (2) Pennsylvania is simply going to look the other way. Rather than take measures to *stop* child pornography where it is being created, the Pennsylvania legislature has decided simply to shield Pennsylvanians from the distasteful content, but allow the conduct to continue.

The case brought against WorldCom helps to illustrate the point.[45] Apparently, in July 2002 the Attorney General's office identified a number of child pornography sites located on the Internet. Instead of taking *any* action to have those sites removed from the Internet and prosecute the perpetrators, the Attorney General waited two months to bring a legal action against the ISP in September 2002. During those two months, whoever was abusing children to make the child pornography *was continuing to do so*. Moreover, the court action did *nothing* to stop the abuse of the child victims.

One specific web site targeted by the September 2002 Court Order makes the point even more clearly. As noted above, the court order required that WorldCom block Pennsylvanians' access to the URL "www.terra.es/personal8/jenout/."[46] Yet a momentary review of the homepage of www.terra.es reveals that the hosting Spanish ISP has a specific abuse reporting procedure *focused on child pornography*. The home page exhorts all terra.es users to cooperate in the fight against child pornography (*Coopera con nosotros contra la pornografía infantile*, which translates to "Cooperate with us against child pornography"), and links to an e-mail address (abuse@terra.es) to be used to report child pornography to the terra.es ISP.[47]

Thus, had the Pennsylvania Attorney General sent a two sentence e-mail reporting the offending URL to the hosting ISP (terra.es in Spain), that ISP could have (a) made the web site inaccessible *to the entire world* (not just Pennsylvania), and (b) reported the operators of the web site to local Spanish authorities for prosecution.

---

[44] *See* Ashcroft, 535 U.S. at ___ (slip opinion at 12) (the Court "anchored" its prior rulings upholding child pornography laws on the concern for the child "victims").

[45] To be clear, the repeated reference to WorldCom in this document arises only because that is the only company to seek to have the Attorney General follow the Pennsylvania statute as written. The actions taken by the Attorney General against other ISPs have all been taken in secret.

[46] Court Order, page 2.

[47] *See* www.terra.es and www.terra.es/p.htm.

Instead, the Attorney General (a) waited until September to take any action, (b) only sought to block access in Pennsylvania to the site, and (c) allowed the site to continue to make child pornography available to the rest of the world not reached by the court order against WorldCom.

No country in the world approves of or permits child pornography. Thus, no ISP in the world can avoid taking action against child pornography if it is brought to their attention. By focusing on local ISPs – that have no involvement whatsoever with the child pornographers – the Pennsylvania legislature chose to allow child pornography to continue unhindered around the world, so long as Pennsylvanians do not see it. That legislative choice was misguided. If the Office of the Pennsylvania Attorney General had spent its efforts on attacking child pornography *at its source* (by contacting the hosting ISPs and the local authorities who have jurisdiction over the child pornographers), those efforts would have a far more significant impact on the problem. Instead, Pennsylvania simply chose to look the other way.

Moreover, by imposing secret censorship orders that reach far outside of Pennsylvania, the Attorney General's actions may actually have *hindered* on-going law enforcement efforts to stop child pornography at its source. The national operations center for all anti-child pornography efforts of the Federal Bureau of Investigation is located outside of Baltimore, Maryland. Any secret blocking order imposed by the Pennsylvania Attorney General on national ISPs like WorldCom would have certainly have blocked access within the adjacent state of Maryland. Thus, it is certainly plausible that an FBI agent could be investigating a distributor of child pornography, and then have the web site apparently disappear from the Internet (as a result of a secret Pennsylvania blocking order). The FBI agent might well assume that the web site had been removed from the Internet, when in fact the web site still operated but was just invisible to a part of the Internet.

Without question, the fight against child pornography should be a critical governmental priority. As the above discussion makes clear, however, the Pennsylvania ISP Liability Law is an unconstitutional and ultimately misguided attempt to achieve that goal. Pennsylvania should focus its law enforcement resources on working with the on-going international law enforcement efforts seeking to combat child pornography *at its source*. A focus on Pennsylvania ISPs that have nothing to do with the child pornographers is both inappropriate and wholly ineffective at protecting the real victims of child pornography.

III. LOOKING BEYOND THE PENNSYLVANIA LAW, ANY GOVERNMENTAL POLICY OF BLOCKING CONTENT BY BLOCKING URL'S AND IP ADDRESSES WOULD RAISE ADDITIONAL CONSTITUTIONAL AND TECHNICAL PROBLEMS

As discussed above, the Pennsylvania ISP Liability Law is plainly unconstitutional. Beyond the myriad problems identified above, however, the basic idea underlying the Pennsylvania law – to use governmental orders to ISPs to block websites that operate elsewhere on the Internet – raises serious *additional* concerns. Any approach using URL- or IP-specific blocking orders will raise at least three serious problems:

First, URL- or IP-specific blocking would raise additional First Amendment concerns. Because URL- or IP-specific blocking schemes cannot, as a technical matter, be limited to the confines of a single state or jurisdiction, serious First Amendment problems would be raised by any state or local effort to regulate speech through such blocking schemes. An important tenet of First Amendment jurisprudence is that the most conservative state or locality in the country cannot impose its views on acceptable content on other others outside of the state or locality. Thus, speech in the United States (including speech on the Internet) cannot and should not be reduced to the "lowest common denominator," allowing a conservative jurisdiction to dictate what content a more liberal jurisdiction can access. But, that is exactly what would happen if states and local governments were permitted to order ISPs to block certain web sites.

Second, URL- or IP-specific blocking would raise constitutional concerns under the Commerce Clause. Again, because URL- or IP-specific blocking schemes cannot, as a technical matter, be limited to the confines of a single state, a state or local imposition of such a scheme would almost certainly violate the Commerce Clause of the United States. Internet communications are plainly "interstate" and have been easily held by courts to be covered by the Commerce Clause (which governs regulation of interstate commerce). If, for example, Pennsylvania ordered a major ISP to block access to a web site that originates in New York State, that action by Pennsylvania would prevent a citizen of Delaware from accessing the New York web site. This would violate accepted constitutional principles under the Commerce Clause, which prevents one state (Pennsylvania) from regulating a transaction that occurs entirely outside of the state's borders (the communication between the Delaware citizen and the New York web site).

Third and finally, a URL- or IP-specific blocking scheme cannot scale. Simply put, if fifty states in the U.S. create blocking schemes like Pennsylvania's, ISPs would be faced with manipulating their "routing tables" in response to hundreds or thousands of blocking orders. As discussed in the factual section above, such a

scenario would create enormous technical risks for the ISP's networks, and the Internet in general. Thus, at the very time when the United States is seeking to improve the reliability and security of its critical infrastructure (including the Internet), Pennsylvania-style blocking schemes, if adopted or used broadly, would seriously threaten that reliability.

IV. CONCLUSION

It cannot be repeated too frequently: no civilized society should permit child pornography, and no one doubts the value of efforts to fight child pornography. The Pennsylvania ISP Liability Law, however, attempts to pursue those laudable goals though unconstitutional, misguided, and technically problematic means. Powerful laws to combat child pornography are in place – all over the world – and those laws should be enforced to their fullest extent. If the Pennsylvania Attorney General identifies child pornography on the Internet, that office should work with the *hosting* ISP and local authorities to identify and prosecute the creators and distributors of child pornography.