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

CENTER FOR DEMOCRACY & TECHNOLOGY, On Behalf of Itself; AMERICAN CIVIL LIBERTIES UNION On Behalf of Its Members; and, PLANTAGENET, INC., On Behalf of Itself and Its Customers	:	**CIVIL ACTION**
Plaintiffs,	:	
vs.	:	**NO. 03-5051**
GERALD J. PAPPERT, Attorney General of the Commonwealth of Pennsylvania	:	
Defendant.	:	

DuBois, J. **September 10, 2004**

TABLE OF CONTENTS

I. INTRODUCTION 3
II. PROCEDURAL HISTORY 5
III. FINDINGS OF FACT 6
A. PARTIES 6
1. Center for Democracy and Technology 6
2. American Civil Liberties Union of Pennsylvania 7
3. PlantageNet, Inc. 7
4. Gerald J. Pappert 7
B. INTERNET OVERVIEW 8
1. Technical Overview of the Internet and the World Wide Web 8
2. Publishing to the World Wide Web 9
3. Domain Names and URLs 11
4. Browsing the Web 13
5. Shared Domain Names 14
6. IP Addresses and the Domain Name System 16
C. INTERNET CHILD PORNOGRAPHY ACT ("THE ACT") 19
1. Implementation of the Act 21
2. The First Complaint 24
3. Informal Notices 25
4. The Single Court Application 29
D. PLAINTIFFS' STANDING 32
E. ISP COMPLIANCE WITH COURT ORDERS OR INFORMAL NOTICES 34

1. Description of ISPs . . . 34
2. Methods of Implementation . . . 36
a. DNS Filtering . . . 36
b. IP Filtering . . . 37
c. URL Filtering . . . 37
3. Comparison of Filtering Methods . . . 37
a. Ease of Implementation and Cost . . . 37
b. Relative Effectiveness . . . 42
c. Overblocking . . . 45
4. Contacting the Host . . . 47
5. Specific Examples of ISP Compliance . . . 51
6. Blocking of Innocent Web Sites . . . 54
a. Laura Blain . . . 55
b. Evidence of Other Blocked Sites . . . 58
7. Notice and Review of Blocked Content . . . 63
8. Methods of Evasion . . . 65
a. Anonymous Proxy Servers . . . 65
b. The Ability of Child Pornographers to Evade Filters . . . 67
9. Office of the Attorney General Response to Overblocking . . . 69
F. IMPACT OF THE ACT ON INTERSTATE COMMERCE . . . 70
IV. CONCLUSIONS OF LAW . . . 71
A. STANDING . . . 71
1. CDT and ACLU . . . 71
2. PlantageNet . . . 74
3. Overbreadth . . . 74
B. SUBSTANTIVE FIRST AMENDMENT ISSUES . . . 76
1. Burden on Speech . . . 77
2. Level of Scrutiny . . . 82
C. PROCEDURAL FIRST AMENDMENT ISSUES . . . 89
1. Prior Restraint . . . 89
2. Child Pornography vs. Obscenity . . . 94
3. Informal Notices . . . 96
D. INTERSTATE COMMERCE CLAUSE . . . 97
1. Pike Balancing Test . . . 99
2. Per Se Invalidity . . . 100
V. CONCLUSION . . . 102
APPENDIX A, 18 Pa. Cons. Stat. §§ 7621-30, Internet Child Pornography Act . . . 102
APPENDIX B, 18 Pa. Cons. Stat. § 6312, Sexual Abuse of Children . . . 106

MEMORANDUM

I. INTRODUCTION

In February of 2002, Pennsylvania enacted the Internet Child Pornography Act, 18 Pa. Cons. Stat. §§ 7621-7630, ("the Act"). The Act requires an Internet Service Provider ("ISP") to remove or disable access to child pornography items "residing on or accessible through its service" after notification by the Pennsylvania Attorney General. It is the first attempt by a state to impose criminal liability on an ISP which merely provides access to child pornography through its network and has no direct relationship with the source of the content. See Jonathan Zittrain, Internet Points of Control, 44 B.C.L. Rev. 653, 654, 672-73 (2003).

The plaintiffs are Center for Democracy and Technology ("CDT"), the American Civil Liberties Union of Pennsylvania ("ACLU"), and Plantagenet, Inc. CDT is a non-profit corporation incorporated for the purpose of educating the general public concerning public policy issues related to the Internet. The ACLU is a non-partisan organization of more than 13,000 members dedicated to defending the principles of liberty and equality embodied in the Bill of Rights. Plantagenet, Inc., is an ISP that provides a variety of services related to the Internet. Defendant is Gerald J. Pappert, Attorney General of the Commonwealth of Pennsylvania.

Plaintiffs argue that, due to the technical limitations of the methods used by ISPs to comply with the Act, the efforts of ISPs to disable access to child pornography in response to requests by the Attorney General have led to the blocking of more than one and a half million innocent web sites not targeted by the Attorney General. Plaintiffs filed suit claiming that this blocking of innocent content, or "overblocking," violates the First Amendment to the Constitution. They also argue, inter alia, that the procedures provided in the Act for issuing an

order to remove or disable access to child pornography are insufficient and allow for an unconstitutional prior restraint of speech. Moreover, they contend that the Informal Notice procedure developed by defendant in implementing the Act also operated as a prior restraint of speech. Finally, plaintiffs claim the Act places an impermissible burden on interstate commerce. Based on these allegations, plaintiffs ask the Court to declare the Act unconstitutional and provide related injunctive relief.

Defendant responds by arguing that the suppression of protected speech is not required by the Act and is the result of action taken by ISPs. According to defendant, ISPs have options for disabling access that would not block content unrelated to child pornography. Defendant also contends that the statutory procedures included in the Act and the Informal Notice procedure adopted by defendant in implementing the Act provide sufficient protection for the removal of child pornography from circulation. Additionally, defendant claims that the Informal Notices did not result in the prior restraint of speech because this procedure was developed with ISP input to provide for an informal and noncoercive means of advising ISPs that child pornography was accessible through their service. Finally, defendant asserts that the Act does not violate the Commerce Clause because child pornography is not commerce.

Based on the evidence presented by the parties at trial, the Court concludes that, with the current state of technology, the Act cannot be implemented without excessive blocking of innocent speech in violation of the First Amendment. In addition, the procedures provided by the Act are insufficient to justify the prior restraint of material protected by the First Amendment and, given the current design of the Internet, the Act is unconstitutional under the dormant Commerce Clause because of its affect on interstate commerce.

The elimination of child pornography is an important goal and those responsible for the creation or distribution of child pornography should be prosecuted to the full extent of the law. To that end, all of the ISPs involved in the case have given defendant their complete cooperation. Notwithstanding this effort, there is little evidence that the Act has reduced the production of child pornography or the child sexual abuse associated with its creation. On the other hand, there is an abundance of evidence that implementation of the Act has resulted in massive suppression of speech protected by the First Amendment. For these reasons, and the other reasons set forth in the Memorandum, the Court is ineluctably led to conclude the Act is unconstitutional.

II. PROCEDURAL HISTORY

On September 9, 2003, plaintiffs filed a Complaint for Declaratory and Injunctive Relief and a Motion for a Temporary Restraining Order and Expedited Discovery. The Complaint alleged that the Informal Notices, which plaintiffs called "secret blocking orders," and the Act violated the First Amendment of the United States Constitution by operating as a prior restraint, burdening a substantial amount of lawful speech, establishing a system of secret censorship, and failing to provide adequate procedural protections. Plaintiffs also alleged that the Act's "significant harmful effect on interstate commerce" violated the Commerce Clause of the Constitution. The Complaint sought an injunction against the Informal Notice process and a declaration that the Act and the Notices issued under the Act were unconstitutional. The Motion asked the Court to enjoin defendant from issuing Informal Notices. By agreement of the parties, the Court entered an Order enjoining the further issuance of Informal Notices and placing limitations on the implementation of the Act by the Attorney General. Pls.' FOF ¶ 5, Order of Sept. 9, 2003. Thereafter, plaintiffs filed a Motion for Declaratory Relief and for Preliminary and

Permanent Injunctive Relief on December 12, 2003 that essentially sought the same relief as was sought in the Complaint. A hearing on this Motion commenced on January 6, 2004. Based on an agreement between the parties, the hearing on the Motion for Declaratory Relief and Preliminary Injunctive Relief was consolidated with a trial on the merits by Order dated March 1, 2004. Because of the schedule of the Court and the parties, the trial continued over twelve non-consecutive days before it concluded with oral argument on June 23, 2004. Following the trial, the parties submitted supplemental memoranda and post-trial proposed findings of fact.

III. FINDINGS OF FACT

The Court's Findings of Fact are made pursuant to Fed. R. Civ. P. 52(a). Where noted, the Findings of Fact are derived from stipulations of the parties. A general overview of the development, architecture, and content of the Internet can be found in Reno v. ACLU, 521 U.S. 844, 849-53 (1997), and will be covered in this Memorandum only to the extent necessary to explain the evidence and the rulings of the Court.

A. PARTIES

1. Center for Democracy and Technology

1. Center for Democracy and Technology ("CDT") is a non-profit corporation incorporated under the laws of the District of Columbia, with its principal office in the District of Columbia, for the purposes of educating the general public concerning public policy issues related to the Internet, conducting legal and policy research concerning the Internet, and developing and advocating public policies to advance constitutional civil liberties and democratic values in connection with the development of the Internet. CDT sues on its own behalf. Jt. Stip. ¶ 1.

2. American Civil Liberties Union of Pennsylvania

2. Plaintiff American Civil Liberties Union of Pennsylvania ("ACLU") is a nonpartisan organization of more than 13,000 members dedicated to defending the principles of liberty and equality embodied in the Bill of Rights. The ACLU is incorporated in Pennsylvania and has its principal place of business in Philadelphia. The ACLU sues on its behalf and on behalf of its members who use online communications. Jt. Stip. ¶ 2.

3. PlantageNet, Inc.

3. PlantageNet, Inc., a Pennsylvania corporation with its principal place of business in Doylestown, Pennsylvania, is an ISP. Def.'s Supp. Mem. at 8. It has a World Wide Web home page at http://www.pil.net. Jt. Stip. ¶ 3.

4. PlantageNet provides its approximately 750 customers with access to the Internet through dial-up, ISDN lines, or dedicated T1 connections. It also hosts customer's web sites on the World Wide Web. Pls.' Finding of Fact ("FOF") ¶¶ 18, 19, Tr. 1/7/04 (Smallacombe) pp. 76-77, 81-83.

4. Gerald J. Pappert

5. The original Complaint named Michael Fisher, then the Attorney General of the Commonwealth of Pennsylvania, as the sole defendant. Upon Mr. Fisher's resignation from that position on December 15, 2003, Gerald J. Pappert became Attorney General and was automatically substituted as the defendant in this action. Mr. Pappert, as Attorney General, has certain powers and responsibilities under the Act that are challenged in this action. Also, as Attorney General, Mr. Pappert heads the Office of Attorney General ("OAG"), and, in his official capacity, is ultimately responsible for the actions of that agency regarding the Informal Notices of

Child Pornography challenged by plaintiffs. Jt. Stip. ¶ 4.

B. INTERNET OVERVIEW

1. Technical Overview of the Internet and the World Wide Web

6. The Internet is a global "network of networks" that allows Internet users to send and receive a huge diversity of content and communications. The "World Wide Web" is a common method that Internet users can use to make content available to other Internet users. Jt. Stip. ¶ 6.

7. In the United States, most people access the Internet through ISPs. Home Internet users generally contract on a monthly or annual basis with an ISP and will access that ISP's network over a dial-up telephone line, or a higher-speed connection such as a cable or digital subscriber line ("DSL"). A typical ISP's network is in turn connected, directly or indirectly (through a larger ISP), to the network of an Internet backbone provider (a very large ISP with high-speed transcontinental or global data lines), and through the backbone to other backbones, ISPs, and networks that, collectively, comprise the global Internet. Jt. Stip. ¶ 7.

8. Businesses in the United States commonly contract with an ISP to provide Internet access to their employees or to connect their internal computer network to the ISP's network, which is in turn connected to the global Internet. Some businesses connect to their ISP's networks (and the Internet) over dedicated high-speed connections, while other businesses access the Internet over dial-up telephone lines, cable circuits, or DSL circuits. Jt. Stip. ¶ 8.

9. A communication over the Internet will commonly travel up the "tree" or hierarchy of networks of one or more backbone providers and then back down to its destination. A hypothetical communication (from an employee of a corporation) might originate on the user's computer, travel through the corporation's network, then through a regional ISP's

network, then to a backbone provider, then to another backbone provider, then back down to a regional ISP, then, in some cases, through the network of a smaller ISP, and then to the corporate network of the destination, and finally to the computer of the intended recipient of the communication. Pls.' FOF ¶ 34; Tr. 1/6/04 (Marcus) pp. 66-67; Pls.' Ex. 2 (Marcus Expert Presentation) at 1.

10. The Act is the first attempt by a state to impose liability on an ISP that does not directly contract with the originator of a communication. Thus, Pennsylvania is the first state to impose liability on, for example, the backbone providers or regional ISPs that route the communication in the hypothetical example in Finding of Fact 9.

11. Some communications on the Internet are divided into small "packets" that are separately sent over the Internet and reassembled on the receiving end. Pls.' FOF ¶ 36; Tr. 1/6/04 (Marcus) pp. 68-69; Tr. 2/26/04 (Marcus) pp. 33-34. Separate packets that make up a given communication on the Internet are not required to travel over the same path from the sender to the recipient of the communication but can be routed over different paths within an ISP's network, or in the middle of the Internet, based on a variety of factors such as congestion on the network. Pls.' FOF ¶ 38; Tr. 1/6/04 (Marcus) pp. 70-71.

2. <u>Publishing to the World Wide Web</u>

12. Individuals, businesses, governments, and other institutions that want to make content broadly available over the Internet (hereafter "web publishers") can do so by creating a web site on the World Wide Web. Jt. Stip. ¶ 9.

13. To make a web site available on the World Wide Web, a web publisher must place the content or web pages onto a computer running specialized web server software. This

computer, known as a Web Server, transmits the requested web pages in response to requests sent by users on the Internet. Jt. Stip. ¶ 10.

14. Web publishers have two common options for making a web site available over a Web Server. First, a web publisher can own and operate a Web Server on the web publisher's premises (including, possibly, the web publisher's home). In that case, the web publisher would contract with an ISP for Internet access and would thereby connect the Web Server to the Internet. Jt. Stip. ¶ 11.

15. Second, a web publisher may contract with a web host (or web hosting company) to own and operate the necessary Web Server on the web host's premises (or third party premises arranged by the web host). A web host will typically operate one or more Web Servers that can store web pages for customers and make those web pages generally available to users on the Internet. Many ISPs offer web hosting services, but many web hosts operate independently of ISPs. Jt. Stip. ¶ 12.

16. A web host offers a web publisher the ability to post a web page or a web site to the World Wide Web. There are a variety of forms of web hosting, including arrangements where a web hosting company: (1) provides a Web Server to service a single web site of a customer, (2) provides a Web Server the customer can use to run multiple web sites, or (3) provides space on a Web Server that services the web sites of many different customers. The third form of web hosting is commonly called virtual web hosting. Pls.' FOF ¶¶ 84, 86; Tr. 1/7/04 (Clark) pp. 178-81.

17. To access web pages on a web site, an Internet user utilizes a client computer program called a web browser. Microsoft Explorer and Netscape are two common web browsers. A web

browser sends a request to a Web Server, which responds by sending the requested web page, which upon receipt is formatted and displayed by the web browser. Pls.' FOF ¶ 43; Tr. 1/6/04 (Marcus) p. 72-73.

3. Domain Names and URLs

18. Typically, but not always, when creating a web site, a web publisher obtains a domain name that can be used to designate and locate the web site. For example, defendant obtained the domain name "attorneygeneral.gov" for his web site. Jt. Stip. ¶ 13.

19. At a minium, a domain name contains a top level domain name and a second level domain name. The following are some top level domains available in the United States: .com, .net, .org, .edu, .gov, .biz, .info. Most nations in the world also have country top level domains, such as us (United States), uk (United Kingdom), es (Spain), it (Italy), ru (Russian Federation). The second level domain appears to the left of the top level domain, separated by a dot. One acquires a domain name (top level and second level) by purchasing it from, and registering it with, a registrar designated for the relevant top level domain, or, alternatively, by purchasing it from someone who already owns the name and offers it for sale. The owner of a domain may create sub-domains that are identified to the left of the second level domain and separated from it by a dot, e.g., subdomain.attorneygeneral.gov. Tr. 1/29/04 (Stern) pp. 32 -33; 2/18/04 (Stern) pp. 58, 106-108; 3/1/04 (Stern) p. 106; Tr. 1/6/04 (Marcus) p. 76; Tr. 1/7/04 (Clark) pp. 137, 151, 154, 156; Tr. 3/1/04 (Blaze) p. 58.

20. Domain names are read right to left. The part of a domain name furthest to the right (or the top level domain) is the broadest part of the domain name. As the domain name is read to the left, the sub-domains identify specific Web Servers or web sites. For example, "upenn.edu" is a sub-

domain of the .edu top level domain identifying the University of Pennsylvania's Web Server, and "cis.upenn.edu" is in turn a sub-domain of upenn.edu used to identify a web site for the Department of Computer and Information Science at the University of Pennsylvania. Pls.' FOF ¶ 45; Tr. 1/6/04 (Marcus) p.76.

21. A domain name can be coupled with additional information to create a Uniform Resource Locator ("URL") which is a more complete way to designate certain content or other resources on the Internet. Jt. Stip. ¶ 14.

22. A URL is the commonly used textual designation of an Internet web site's address. Thus, for example, the URL of defendant's web site is http://www.attorneygeneral.gov. The http indicates that the Hypertext Transfer Protocol (which is the main protocol used to transmit World Wide Web pages) is to be used. The "www.attorneygeneral.gov" part of the URL is used to locate the specific Web Server(s) that contains (hosts) the content for the requested web site. Jt. Stip. ¶ 15.

23. A web page accessed by a URL like http://www.attorneygeneral.gov is commonly referred to as the home page of the web site. A URL can also contain a reference to a specific sub-page contained in a web site. The sub-page is designated in writing by slashes after the home page (such as http://www.attorneygeneral.gov/press/pr.cfm). A single web site can contain thousands of different web pages. Jt. Stip. ¶ 16.

24. A URL on the World Wide Web only refers to a location where content can be found. A URL does not refer to any specific piece of static content – the content is permanent only until it is changed by the web site's webmaster (often, but not always, the owner of the web site). The actual content to which a URL points can (and often does) easily change without the URL

changing in any way. Pls.' FOF ¶ 53; Tr. 1/6/04 (Marcus) p. 77; Tr. 1/6/04 (Blain) pp. 26-28.

4. Browsing the Web

25. For accessing content on the World Wide Web, the most common sequence is for a user to request content from a web site, and for the web site to return web pages to the user. This sequence is illustrated as follows, with the initial request shown by the arrows on the left, and the response shown by the arrows on the right:

User

↓ ↑

User's ISP

↓ ↑

Internet "Backbone" Provider(s)

↓ ↑

Web Site's ISP

↓ ↑

Web Site

Jt. Stip. ¶ 22.

26. In the vast majority of cases, the user's ISP is different from the web site's ISP. Jt. Stip. ¶ 23.

27. To access a web page, a user can either type the URL of the web page into his web browser, or, if the user is already accessing a web page, click on a hyperlink that takes the user to a different web page. A hyperlink is commonly shown on a web page with underlining; for example, on a web listing of the University of Pennsylvania Department of

Computer and Information Science faculty members, an individual professor's name would be underlined and clicking on the name would take the user to the professor's personal web page. Pls.' FOF ¶ 57; Tr. 1/6/04 (Marcus) pp. 78-79.

5. Shared Domain Names

28. Within the United States alone, there are tens of millions of separate domain names used for web sites that are, for the most part, independent of each other. In the great majority of those situations, a single web publisher controls the domain name and the entire web site and is responsible for all pages and sub-pages on a web site. Thus, www.example.com could be the fully qualified domain name for a single web site (with multiple pages) controlled, hypothetically, by the Example Corporation. This approach – of a single web site being coextensive with the domain name – is the most familiar approach to placing content on the web. Jt. Stip. ¶ 17.

29. Web publishers can also publish on the World Wide Web without obtaining their own unique domain names for their web sites. For example, a web publisher can place content with a provider that offers to host web pages on the provider's own web site (as a sub-page under the provider's domain name). Thus, hypothetically, the Example Corporation could have a web site at the URL http://www.webhostingcompany.com/example. Some such providers offer their users discussion forums, chatrooms, and other services and are known more broadly as online communities. Jt. Stip. ¶ 18.

30. GeoCities is an example of an online community located in the United States. GeoCities hosts web pages of its users as sub-pages of its domain name. As an illustration, the Association of Black Women Lawyers of New Jersey, Inc., is part of the GeoCities online community, and its

web pages are available at the URL http://www.geocities.com/abwlnj/homepage.html. Jt. Stip. ¶ 19.

31. OAG staff members refer to "an entity or person that permits other persons to post their own sites or content as sub-pages under the single domain name of the host such as GeoCities.com, terra.es, or PhotoIsland.com" as a Web Hosting Service. Pls.' Ex. 73 (Def.'s Ans. to Pls.' Third Req. for Prod. of Docs. and Interrogs.) ¶ 12; Tr. 1/9/04 (Guzy Sr.) p. 72.

32. Outside of the United States, www.terra.es is a well-known Spanish-language online community providing web hosting services. Jt. Stip. ¶ 20.

33. Some web hosts allow users to create web sites using individualized subdomains of the web hosts' primary domain. Thus, hypothetically, the Example Corporation web site might be at the URL http://example.webhostingcompany.com, while another customer site might be at the URL http://acehardware.webhostingcompany.com. Jt. Stip. ¶ 21.

34. Other than their existence as sub-pages or sub-domains on a providers' domains, web sites hosted as sub-pages or sub-domains are usually independent of the provider and independent of each other. Tr. 1/29/04 (Stern) pp. 54-59; 2/18/04 (Stern) pp. 103, 104.

35. Many web hosting companies offer to host web sites at a very low cost and often theses hosts offer virtual hosting – they host sites on a single Web Server. Some such web hosting companies offer to host web sites at no charge in exchange for the right to place advertisements for their service on the customer's web site. Pls.' FOF ¶ 96, Tr. 1/6/04 (Blain) pp. 26-30 (describing creation of free and low-cost web sites for two community organizations); Tr. 1/7/04 (Smallacombe) pp. 81-83, 100-102.

6. IP Addresses and the Domain Name System

36. A URL such as http://www.attorneygeneral.gov or http://www.geocities.com/abwlnj/homepage.html provides enough information for a user to access the desired web site. The user enters the URL in her web browser. However, the URL alone is not sufficient for the user's computer to locate the web site. A user's computer must first determine the numeric Internet Protocol Address or IP address of the desired web site. Every device, or computer, using the Internet must have a unique IP address.

37. When a user seeks to access a particular URL, the user's computer initiates a look up through a series of global databases known as the domain name system ("DNS") to determine the IP Address of the Web Server that can provide the desired web pages. Jt. Stip. ¶ 24, Tr. 1/29/04 (Stern) p. 36- 40. To search for the requested URL's IP address, the user's web browser must query a domain name system server ("DNS server") that has been assigned or selected within the user's computer. That DNS server attempts to find the IP address of the fully qualified domain name specified in the URL entered by first looking in its own database of domain name/IP address combinations. If that DNS server cannot find the IP address in its own database, it queries other DNS servers until it receives the correct IP address. It then returns that address to the user's computer. This process is referred to as resolving a hostname to its IP address. Jt. Stip. ¶ 25.

38. Typically, an ISP gives its customers the IP addresses of DNS servers controlled by the ISP. The addresses are entered in the customers' computers during the Internet access set-up process, a process that is often automated. Some ISPs assign a new IP address identifying a different DNS server each time the user establishes a connection to the ISP. This is called dynamic assignment. Tr. 1/29/04 (Stern) p. 36; Tr. 1/7/04 (Marcus) pp. 5-7; Tr. 1/7/04 (Smallacombe) pp. 113-114;

Tr. 1/27/04 (MacDonald) pp. 144-148.

39. Companies and other network operators can choose to operate their own DNS servers. Pls.' FOF ¶ 65, Tr. 1/6/04 (Marcus) p. 84. Individuals can also chose not to use the DNS server assigned by their ISP and can either use a DNS server available on the Internet or operate their own DNS server. Tr. 1/6/04 (Marcus) pp. 83-84, 116.

40. The numeric IP address of the DNS server provides the user's computer with the Internet address of the Web Server to which the user's computer then sends a request for the particular URL entered in the user's web browser. IP addresses (in the most common current form) are generally expressed as four sets of numbers separated by periods, e.g., 207.102.198.176. Jt. Stip. ¶ 26.

41. IP addresses are assigned by several registries covering various parts of the world. Tr. 1/29/04 (Stern) p. 37. The party to whom the registry assigns an IP address may subassign the address. The sub-assignment may, but need not, be recorded with the registrar. The sub-assignee may further sub-assign the IP address. Tr. 1/27/04 (Krause) pp. 119-120; Tr. 1/28/04 (Clark) pp. 152-160; Tr. 1/12/04 (Guzy Jr.) pp. 36, 60-62, 181, 182.

42. Although a specific URL refers only to one specific web site, many different web sites (each with different domain names and URLs) are hosted on the same physical Web Server, and all the web sites on a server share the same IP Address. Jt. Stip. ¶ 27.

43. It is common for web hosting companies to offer virtual web hosting, discussed in Finding of Fact 16, under which many web sites are hosted on the same Web Server and thus share the same IP address. Pls' FOF ¶ 72; Tr. 1/6/04 (Marcus) p. 94; Pls.' FOF ¶ 73; Tr. 1/29/04 (Stern) p. 65; Dep. of G. Lipscomb (Comcast) at 115-16; Dep. of C. Silliman (WorldCom) at 103 (anecdotally

from general industry information, it is believed that the majority of web sites share IP addresses with more than 50 sites). As an example of virtual web hosting, PlantageNet hosts about 160 to 170 of its web hosting customers – all with their own unique domain names – on a single Web Server with a single IP address. Tr. 1/7/04 (Smallacombe) pp. 82-83. As another example, discussed more fully below, Laura Blain's web site shared its IP address with more than 15,000 other domains. Tr. 1/7/04 (Clark) pp. 141-42.

44. Research by plaintiffs' expert Michael Clark empirically confirms the prevalence of shared IP addresses. In October - November 2003, Mr. Clark created a database of 29.5 million domain names and the IP addresses to which each domain named resolved. Using this database, which was received in evidence in CD-ROM form as Plaintiffs' Exhibit 77, Mr. Clark analyzed the frequency with which IP addresses were shared among domain names. Pls' FOF ¶¶ 76. Tr. 1/7/04 (Clark) pp. 134-35, 137-40, 151-60, 170-71. In Joint Stipulation 59, the parties agreed that, for a variety of reasons, it is difficult to state a precise percentage of domain names that share an IP address with other domain names. However, they agreed and stipulated that "at the time the data was collected (October 2003), at least fifty percent of domains shared an IP address with at least fifty other domains." Pls.' FOF ¶ 78; Jt. Stip. ¶ 59. Some domains do not share IP addresses with other domains but are the only domain located at a single IP address. As of October 2003, over 2.5 million domains had their own, unshared, IP addresses. Jt. Stip. ¶ 59.

45. When a request for a web site reaches a Web Server that supports multiple web sites, the Web Server reads the request, including the IP address and the URL, in order to determine which web site is being requested, and returns only the requested web page or other resource. Jt. Stip. ¶ 28.

46. When a request for a particular web page is sent by the user's web browser to a Web Server, no ISP that carries the request must read the details of the request – an ISP routing the request is only required to read the destination IP address, and the ISP would effectively not be aware of the specific web site or URL requested. Pls.' FOF ¶ 70; Tr. 1/6/04 (Marcus) pp. 92-93.

47. One cannot determine with any certainty – using technical means – whether a given web site shares its IP address with another web site. The most reliable method of determining whether a particular web site uses an IP address shared by other web sites is to contact the web hosting entity. Tr. 1/7/04 (Clark) pp.182-83. As Mark Krause, Senior Manager of Internet Infrastructure Security for WorldCom/MCI, explained, it is "hard, or impossible for [an ISP] to determine what other content" might be behind a particular IP address. Pls.' FOF ¶ 80; Tr. 1/27/04 (Krause) pp. 9, 98.

C. INTERNET CHILD PORNOGRAPHY ACT ("THE ACT")

48. On February 21, 2002, Pennsylvania enacted the Internet Child Pornography Act, codified at 18 Pa. Cons. Stat. § 7330 and effective in 60 days (April 22, 2002) ("the Act"). On December 16, 2002, the Act was recodified at 18 Pa. Cons. Stat. §§ 7621-7630, without change in substance. Jt. Stip. ¶ 29.[1]

49. The Act permits defendant or a district attorney in Pennsylvania to seek a court order requiring an ISP to "remove or disable items residing on or accessible through" an ISP's service upon a showing of probable cause that the item constitutes child pornography. The application for a court order must contain the Uniform Resource Locator providing access to the item. Pls.' FOF ¶¶ 2, 145; 18 Pa. Cons. Stat. §§ 7626-7628.

---

[1]The text of the Act is attached as Appendix A.

50. Child pornography is defined as images that display a child under the age of 18 engaged in a "prohibited sexual act." A prohibited sexual act is defined as "sexual intercourse . . . 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." Pls.' FOF ¶ 141; 18 Pa. Cons. Stat. § 6312.[2]

51. The court order may be obtained on an ex parte basis with no prior notice to the ISP or the web site owner and no post-hearing notice to the web site owner. Pls.' FOF ¶ 142; 18 Pa. Cons. Stat. §§ 7626-7628.

52. Under the Act, a judge may issue an order directing that the challenged content be removed or disabled from the ISP's service upon a showing that the items constitute probable cause evidence of child pornography. A judge does not make a final determination that the challenged content is child pornography. Pls.' FOF ¶ 143; 18 Pa. Cons. Stat. § 7627.

53. Once a court order is issued, the Pennsylvania Attorney General notifies the ISP in question and provides the ISP with a copy of the court order. The ISP then has five days to block access to the specified content or face criminal liability, including fines of up to $30,000 and a prison term of up to seven years. Pls.' FOF ¶ 144; 18 Pa. Cons. Stat. §§ 7624, 7628.

54. According to defendant, the purpose of the Act is: "To protect children from sexual exploitation and abuse. To serve this purpose by interfering with distribution of child pornography, particularly its distribution over the Internet." Pls.' Ex. 75 (Def.'s Resp. to Pls.' Fourth Set of Interrogs.) ¶ 1.

---

[2]The complete text of the statute setting forth this definition of child pornography is attached as Appendix B.

55. Government law enforcement agencies have attempted to locate and criminally prosecute persons who produce or knowingly distribute child pornography. However, a state agency in the United States cannot easily prosecute producers and distributors of child pornography because they are rarely found in that particular state and often are not found in the United States. Tr. 1/9/04 (Burfete) p. 17-19.

1. Implementation of the Act

56. To implement the Act, the OAG formed a Child Sexual Exploitation Unit ("CSEU") and assigned two agents and a supervisory agent to the unit. Starting in late April 2002, these agents investigated complaints by citizens regarding child pornography on the Internet and also searched the Internet for child pornography using ISPs to which the OAG subscribed. From time to time, the OAG changed the ISPs to which it subscribed. The agents worked from locations in Pennsylvania. Jt. Stip. ¶ 30.

57. Special Agent Dennis Guzy Sr. was the supervisory special agent in charge of the unit. The two other assigned agents – Agent Marnie and Agent Ceh – reported to him. Pls.' FOF ¶ 178; Tr. 1/9/04 (Guzy Sr.) pp. 52, 116. The OAG assigned Deputy Attorney General John J. Burfete to be the legal advisor to the CSEU. Def.'s FOF ¶ 141, Tr. 1/8/04 (Burfete) pp. 105-06. Dennis Guzy, Jr., the Manager of Information Resources Development for the Information Technology and Law Section, was assigned as a liaison to the CSEU and provided technical assistance to the unit. Tr. 1/12/04 (Guzy Jr.) p. 10.

58. The OAG created an electronic citizen complaint form for reporting Internet sites displaying child pornography. The OAG posted the form on the OAG's web site. Pls.' Ex. 104 (Collection of Screenshots), tab 4 (Screenshot of complaint form on OAG web site); Def.'s FOF ¶ 140.

59. The OAG subscribed to the following ISPs at various times since April 2002: AOL, Verizon, WorldCom, Microsoft Network, Earthlink, Comcast, and Epix. Jt. Stip. ¶ 31.

60. Soon after the Act was enacted in February 2002, ISPs contacted the OAG to express concern about the Act, its enforcement, and ISPs' fundamental inability to block access to content located outside of their networks. Tr. 1/8/04 (Burfete) pp. 29-32, 39; Pls.' Ex. 7 (3/15/04 e-mail from Burfete describing conversation with AOL); Pls.' Ex. 9 (e-mail from Burfete attached to 3/20/02 e-mail from Guzy Sr. stating "The major complaint is that it is technologically impossible for an ISP to comply with a notice to deny access to a URL to Pennsylvania residents only on which child pornography has been accessed. The ISPs indicate they can deny access to their entire customer base nationwide.") Specifically, the ISPs were concerned that "if the child pornography site is not on their equipment, is not on computers that they run, it becomes very difficult, if not impossible, for them to go in and simply remove the offending child pornography." Pls.' FOF ¶¶ 158, 159; Tr. 1/8/04 (Burfete) p. 39; see also Dep. of C. Bubb (Assistant General Counsel for AOL) at 23.

61. On April 4, 2002, representatives of the United States Internet Service Providers Association and several ISPs met with representatives of the OAG to discuss implementation of the Act. On April 15, 2002, representatives of several ISPs again conferred with representatives of the Attorney General, some in person, some by telephone conference call, regarding implementation of the Act. At these conferences, the participants discussed (1) informal implementation of the Act to avoid issuance of court orders to ISPs, and (2) technical methods of blocking or disabling access to sites accessible through, but not resident on, an ISP's service. Jt. Stip. ¶ 32.

62. At the April 2002 meetings, the ISP representatives stated that they wanted to avoid the

statutory notices based on court orders, which required compliance in five business days and provided criminal sanctions for noncompliance. As a possible solution to that problem, an America On Line ("AOL") attorney, Christopher Bubb, suggested a procedure under which the OAG would informally, without a court order, notify an ISP of child pornography items found residing on or accessible through its service, and the ISP would be given the opportunity to remove the items or disable access. The OAG staff, which had also been considering some kind of informal approach, agreed to implement such an informal procedure. Bubb Dep. pp. 19-21, 28-31, 33-34; Tr. 1/8/04 (Burfete) pp. 38-39, 114-116; Tr. 1/9/04 (Ryan) pp. 215, 228, 229; Tr. 1/9/04 (Guzy Sr.) pp. 116-119; Pls.' Ex. 7 (Mar. 15, 2002 e-mail from Burfete discussing conversation with Bubb); Def.'s FOF ¶ 135.

63. At the April 2002 meetings, representatives of the OAG advanced the use of DNS filtering, URL filtering, and IP filtering as possible methods that ISPs could use to comply with a court order issued under the Act or any informal notice procedure utilized by the OAG. Jt. Stip. ¶ 33; Pls.' FOF ¶ 165; Tr. 1/12/04 (Guzy Jr.) pp. 16-17. Mr. Guzy Jr. did not think "it was [the OAG's] place to say whether one way or another is acceptable, other than that . . . it was up to the ISPs to choose which method. But, certainly any of those three, I believe, would have been acceptable." Tr. 1/12/04 (Guzy Jr.) pp. 74-75.

64. The OAG's identification of possible methods of technical compliance was based solely on testing within the network of the Attorney General's office and not on any testing in an ISP setting. Tr. 1/12/04 (Guzy Jr.) pp.11-12, 22, 26. ISPs raised concerns that the testing was limited in scope in that it was conducted only on the OAG's Local Area Network ("LAN") and did not accurately reflect the problems an ISP operating a national or regional network would encounter

if it tried to implement any of the three filtering methods on a larger scale. Pls.' FOF ¶ 166; Dep. of R. Hiester (Verizon) at 14; Dep. of C. Bubb (AOL) at 35.

65. At no time during the April 2002 meetings did the OAG suggest to the ISPs that they could comply with an informal notice procedure or court order by contacting the web host and having the web host remove the targeted content from its Web Server. The OAG only suggested technical means of compliance during those meetings. Pls.' FOF ¶ 168. Tr. 1/9/04 (Burfete) p. 19; Tr. 1/12/04 (Guzy Jr.) p. 74.

2. The First Complaint

66. In response to the first child pornography complaint to the CSEU, on April 22, 2002, Special Agent Guzy contacted a child pornographer the OAG had identified in Ohio, Pavel Ushakov, and informed him that the OAG had identified child pornography on his web site. Mr. Ushakov was told by Agent Guzy that he could continue his Internet business if he removed the offending images from his web site. Pls.' Ex. 20 (e-mail exchange between Guzy Sr. and Ushakov) at 3; Tr. 1/9/04 (Guzy Sr.) pp. 63-67.

67. The OAG decided to contact Mr. Ushakov directly because "it was a very unique case." The web site he administered was "devoted towards nudism" and included pictures of nude adults and children. Agent Guzy was concerned that "if we followed the normal practice and contacted the ISP and asked them to deny access to the site, it would deny access to the entire site which included the adult male and female nudism pictures which were not in violation of Pennsylvania law." Pls.' FOF ¶ 135; Tr. 1/9/04 (Guzy Sr.) pp. 81-82.

68. The action of the OAG led Mr. Ushakov to remove the child pornography from the Internet. Tr. 1/8/04 (Burfete) p. 62. The OAG did not initiate criminal proceedings against Mr. Ushakov.

Tr. 1/9/04 (Guzy Sr.) pp. 65-67; Tr. 1/8/04 (Burfete) p. 54.

69. With the exception of the Ushakov incident, the OAG did not routinely investigate persons or entities that created, posted or published the child pornography subject to Informal Notices that it issued. Defendant admitted that between March 1, 2003 and September 9, 2003 the OAG did not "use any investigative steps, methods or techniques prior to the issuance of any Informal Notice . . . to determine the identity, address, or location of the individuals or entity that created any alleged child pornography." Pls.' Ex. 73 (Def.'s Answers to Pls.' Third Req. for Prod. of Docs. and Interrogs.) ¶¶ 1-3; Pls.' FOF ¶ 541.

3. Informal Notices

70. Starting in late April 2002, when an agent or citizen complainant identified a suspected child pornography web site and Agent Guzy reviewed the site and concluded that it displayed child pornography, as defined by 18 Pa. Cons. Stat. § 6312, an agent sent a document titled "Informal Notice of Child Pornography" to the ISP through whose service the agent or the citizen complainant had accessed the site. Each Notice identified the URL (or URLs) of the site(s) to which the Notice was directed. Jt. Stip. ¶ 34; Pls.' FOF ¶ 174; Tr. 1/9/04 (Guzy Sr.) pp. 68-69; Tr. 1/8/04 (Burfete) pp. 58-62.

71. The Informal Notices followed a standardized form, which changed somewhat over time. The first form, used from April 2002 until mid-July 2002, read as follows:

> This notice is provided to you under the provision of Section 7330 of the Pennsylvania Criminal Code, 18 PACs 7330, Internet Child Pornography. This notice is further provided to you to advise you that child pornography, as defined at Section 6312 of the Pennsylvania Crime Code, 18 PACs 6312, has been accessed through your service at uniform resource locator http://[redacted].
>
> You must 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 must ensure that: 1. Access to uniform resources locator http://[redacted] be denied to your subscribers to your services from an address located within the Commonwealth of Pennsylvania using Internet services provided by [ISP] and that the Attorney General or his designated agent is notified in writing (e-mail, fax) that you have complied with this Informal Notice within five business days of said compliance. 2. Accompanying this compliance notification should be a screen shot of the resource locator demonstrating that access has been disabled.

Jt. Stip. ¶ 35.

72. From mid-July 2002 through the end of 2002, the Informal Notices omitted reference to Section 7330 of the Act, providing as follows:

> This notice is provided to you to advise you that child pornography, as defined at Section 6312 of the Pennsylvania Crimes Code, 18 Pa. C.S. § 6312, has been accessed though your service at uniform resource locator http://[redacted].
>
> You must 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 must ensure that: 1) Access to uniform resources locator http://[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]; 2) That the Attorney General or his designated agent is notified in writing (e-mail, fax) that you have complied with this Informal Notice within five business days of said compliance; 3) Accompanying your compliance notification to the Office of Attorney General must be a screen shot of the web page accessed by the uniform resource locator demonstrating that access has been disabled.

Jt. Stip. ¶ 36.

73. Beginning in 2003, the OAG changed the form of the Informal Notice of Child Pornography by substituting the word "should" for the word "must" at the beginning of the second and third paragraphs and by adding a sentence at the end of the Notice that referenced the Act. The

Notice, as amended, read as follows:

> This notice is provided to you to advise you that child pornography, as defined at Section 6312 of the Pennsylvania Crimes Code, 18 Pa. C.S. § 6312, has been accessed though your service at uniform resource locator http://[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 resources locator http://[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]; 2) That the Attorney General or his designated agent is notified in writing (either U.S. Mail, e-mail, or facsimile) that you have complied with this Informal Notice within five business days of said compliance; 3) Accompanying your compliance notification to the Office of Attorney General 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 Codes, 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.

Jt. Stip. ¶ 37.

74. Reference to the Act was added to the third version of the Notice after having been removed from the second version because the OAG wanted ISPs to know that, if they failed to comply with an Informal Notice, the OAG could seek a court order under Chapter 76 of the Crimes Code. Pls.' FOF ¶ 185; Tr. 1/8/04 (Burfete) p. 122.

75. The OAG reported each site identified in an Informal Notice to the National Center for Missing And Exploited Children, which acts as a clearinghouse for federal agencies that investigate and prosecute persons who publish and distribute child pornography. Tr. 1/9/04 (Burfete) pp. 16-17; Tr. 1/9/04 (Guzy Sr.) p. 183; Def.'s FOF ¶ 153.

76. Throughout the administration of the informal process, the OAG staff gave the ISPs additional time beyond that stated in the Notices for compliance. Tr. 1/9/04 (Guzy Sr.) p. 137; Tr. 1/8/04 (Guzy Sr.) p. 124. For example, the OAG gave Microsoft a month to comply with Notices sent in June 2002. Tr. 1/9/04 (Guzy Sr.) p. 137; Tr. 1/8/04 (Burfete) pp. 45-47, 124-125. In January 2003, the OAG gave AOL and Verizon additional time to comply with a larger than usual number of notices. Tr. 1/9/04 (Guzy Sr.) p. 138; Tr. 1/8/04 (Burfete) pp. 125-126. Agent Guzy told Comcast representatives that the OAG would work with Comcast regarding the time for compliance. Comcast was given additional time to comply throughout the period notices were sent to Comcast, primarily March to September 2003. Lipscomb Dep. pp. 35-36, 42-43; Tr. 1/9/04 (Guzy Sr.) pp. 137-138.

77. The OAG continued sending Informal Notices of Child Pornography to ISPs until September 9, 2003, when the Court entered the agreed upon injunction. The agents sent approximately 250 Informal Notices to ISPs in 2002 and 220 in 2003. Jt. Stip. ¶ 38. These notices covered approximately 376 distinct URLs. Pls.' FOF ¶ 196; Jt. Ex. 9 (Agreed List of Informal Notices) Tabs B, D; Jt. Stip. ¶ 60.

78. The ISPs generally responded to the Informal Notices by stating, in writing, that they had complied. Jt. Stip. ¶ 39.

79. Excluding notices sent directly to certain Web Hosting Services as referenced in Finding of Fact 208, the vast majority, if not all, of the Informal Notices sent to ISPs related to content that the ISP did not itself host. Jt. Stip. ¶ 40.

80. The Informal Notices were issued in lieu of court orders. No court orders were issued regarding the web sites identified in the Informal Notices. Jt. Stip. ¶ 41.

81. In no instance did the OAG agents inform the owner of targeted web site(s) that her site was being targeted, either before or after an Informal Notice was sent to an ISP. Pls.' Ex. 73 (Def.'s Answers to Pls.' Third Req. for Produc. of Docs. and Interrogs.) ¶¶ 1-3.

82. No court reviewed or approved any Informal Notices or reviewed any of the content addressed in the Notices prior to the issuance of the Notices. Jt. Stip. ¶ 42.

83. AOL viewed Informal Notices as orders with which it must comply and believed it would be prosecuted if it failed to comply. Dep. of C. Bubb at 100-03.

3. The Single Court Application

84. On July 25, 2002, in response to several Informal Notices sent by the OAG, WorldCom, an ISP, wrote a letter to the OAG, stating that it is "absolutely opposed to child pornography, and [it] regularly work[s] with law enforcement in various jurisdictions" to facilitate prosecution of child pornographers. However, WorldCom claimed that it was "not technically-feasible" for it to block access to a site on the Internet based on the URL of that site. WorldCom stated that it would "promptly comply with any court order (or other applicable legal process) relating to your fight against child pornography." Jt. Stip. ¶ 44; Jt. Ex. 2 (July 25, 2002 letter from Craig Silliman).

85. An attorney for WorldCom, Craig Silliman, in conversations with the OAG, expressed "concerns" about the "technical feasibility" of compliance with the Informal Notices received by WorldCom. He also told the OAG "our concern was that although they were citing to the law, that the notice was in fact not sent pursuant to the law. And that it was very important to us that we follow the proper legal process . . . we felt most comfortable acting under that process because the statute did lay out a process." Dep. of C. Silliman (WorldCom) at 58-64.

86. From the July 25, 2002 letter and other communications with WorldCom, the OAG determined that WorldCom intended to comply with any court order by blocking access to IP addresses. Specifically, Mr. Silliman asked that the OAG obtain court orders that identified IP addresses rather than URLs, so that any blocking of content not targeted by the OAG would be done by court order. Pls.' FOF ¶ 217; Dep. of C. Silliman (WorldCom) at 69-71; Jt. Ex. 2 (July 25, 2002 letter from Craig Silliman).

87. In September 2002, the Attorney General filed an Application for an Order Requiring an Internet Service Provider [WorldCom] to Remove or Disable Access to Child Pornography in the Court of Common Pleas of Montgomery County. Jt. Ex. 3 (Application). On September 17, 2002, the Montgomery County Court entered an "Order Requiring an Internet Service Provider to Remove or Disable Access to Child Pornography" ex parte. Jt. Ex. 4 (Court Order), Jt. Stip. ¶ 45. The Court directed WorldCom to deny access to five URLs listed in the Order. Jt. Ex. 4 ¶¶ 2,3. The sites were not identified by IP Address as requested by WorldCom.

88. Before obtaining the court order, the OAG retained a physician to review the alleged child pornography to ensure that the individuals depicted were minors. The OAG did not consult a physician before issuing any Informal Notices. The purpose of consulting with the physician with respect to the WorldCom order was to "make certain . . . that the materials that we saw were indeed child pornography." Tr. 1/9/04 (Burfete) pp. 35-38, 43.

89. On September 17, 2002, the OAG sent WorldCom, by e-mail and overnight mail, a covering letter signed by Mr. Burfete, a Notice of the Application and Order, a copy of the Order, and a copy of the Application. Jt. Stip. ¶ 46.

90. The cover letter stated: "If you determine that one or more of the URL's is indeed the

address of a web hosting service, it may be possible to comply with the Court order and notice by contacting the web hosting service and advising it that a site it is hosting has been found by a Pennsylvania Court to contain child pornography. In the past, web hosting services upon such contact have removed the offending web site. If the hosting service does remove the offending web site, and the site is thereby no longer accessible through WorldCom to Pennsylvania residents, you will have complied with the Court Order and Notice." Jt. Ex. 5 (Sep. 17, 2002 letter from Burfete to Silliman).

91. On September 18, 2002, the OAG issued a press release. Jt. Stip. ¶ 47. The press release stated, "In the vast majority of cases, the ISPs have agreed to disable access to the child pornography site to all of their Pennsylvania customers [in response to an 'informal notification' from the OAG]. . . . [The OAG] notified WorldCom that an agent had discovered child pornography at several Internet sites accessible through World Com. Fisher's agents requested that access to the sites be disabled. However, WorldCom informed the Attorney General's Office that it would not deny access to the child pornography sites." Jt. Ex. 7 (press release).

92. WorldCom informed the OAG that it had complied with the order by letter dated September 23, 2002. Jt. Ex. 8 (Sep. 23, 2002 letter from Silliman to Burfete); Jt. Stip. ¶ 48. WorldCom explained that, for three of the five URLs it identified the hosting ISP through publicly available information, called the appropriate contact listed on the ISPs' web sites, and followed up by sending an email. Those three sites were removed by the web host. Jt. Ex. 8. With regard to the other two sites identified in the court order, WorldCom ultimately instituted a block on the IP addresses associated with the URLs because it was unable to verify that the targeted content had been removed by the host. Id. One of the three web sites contacted by WorldCom was

Terra.es, a large Spanish online community. Dep. of C. Silliman (WorldCom) at 82-83.

93. WorldCom also instituted a process to track the IP addresses of the sites it blocked in response to the court order so that it could change the block if the IP addresses of the targeted URLs were changed. The IP addresses of the sites that WorldCom was ordered to block changed only at two basic time periods (including a number of rapid changes over a weekend). Pls.' FOF ¶ 225; Dep. of C. Silliman (WorldCom) at 97-99.

94. Other than the one application covering sites accessible through WorldCom, the OAG did not file any applications for court orders under the Act. Jt. Stip. ¶ 49.

95. No Pennsylvania district attorney has filed any court application under the Act. Jt. Stip. ¶ 50.

D. PLAINTIFFS' STANDING

96. CDT obtains its Internet access from WorldCom. Pls.' FOF ¶ 11. Tr. 1/27/04 (Clark) at 183.

97. Members of ACLU obtain Internet access from, inter alia, Epix, AOL, and Verizon. A number of these members utilize the Google.com search engine to retrieve information maintained on various web sites, and they are not familiar with the content or the name of these web sites before this information is retrieved by the search. Such members seek access to "the broadest reaches of the Internet." Pls.' FOF ¶ 13; Pls.' Ex. 76 (Verifications of Janet Goldwater, Clark Moeller and Gene Bishop).

98. Janet Goldwater, a member and former board member of ACLU, seeks access to specific web sites that are currently being blocked by her ISP, AOL, as a result of Informal Notices 1086 and 2966. Specifically, Ms. Goldwater attempted to access the following three blocked web sites:

(1) http://isladeesculturas.tuportal.com/page2.html;

(2) http://cazurro.tuportal.com/webs/index.html; and

(3) http://www.movieposterforsale.us/afiliado8.htm.

Pls.' FOF ¶ 14, Tr. 1/28/04 (Goldwater) pp.112-18, Pls.' Ex. 5 (Third Report and Testimony of Michael B. Clark) ¶ 6 (providing IP addresses of the sites Ms. Goldwater sought to access); Jt. Ex. 9 (Agreed Lists of Informal Notices), Tab A, Lines 44 & 92 (listing those same IP addresses as blocked by AOL in response to Informal Notices 1086 and 2966).[3] The Attorney General has acknowledged that these sites do not contain child pornography. Pls.' Ex. 74 (Def.'s Resp. To Pls.' First Set of Reqs. For Admissions) ¶ 1.

99. PlantageNet outsources the Internet access services that it provides to most of its customers. It contracts with a wholesale Internet service provider – Coretel, located in Maryland – to provide the dial-in modems and dedicated connections through which PlantageNet's customers physically access the Internet. The fact that PlantageNet's customers actually connect to the Internet through another ISP is not made known to the customers who would, in most cases, never know that another ISP is involved. Most, if not all, of PlantageNet's customers would conclude that PlantageNet is the only ISP involved in providing their service. Tr. 1/7/04 (Smallacombe) pp. 77-78, 107.

100. The OAG would have sent PlantageNet an Informal Notice or sought a court order if it learned that child pornography was accessible through PlantageNet's service. Mr. Burfete and Special Agent Guzy stated that they viewed PlantageNet as an ISP and PlantageNet was subject to court orders under the Act notwithstanding the fact that it outsourced its Internet access

[3]The transcript contains typographical errors as to the precise web sites that Ms. Goldwater attempted to access. The correct web sites are listed at Pls.' Ex. 5 ¶ 2.

operations. Pls.' FOF ¶¶ 24, 26; Tr. 1/8/04 (J. Burfete) pp. 47-50, Tr. 1/9/04 (Guzy Sr.) pp.124-25.

101. In mid-2002, Microsoft, another ISP that outsources Internet access, asserted that it should not have been the target of Informal Notices because it did not own or operate its own network. In response, John Burfete reported that if an ISP that outsourced, such as Microsoft, was unable to get its third party service providers to comply with a blocking order, the OAG would initiate legal proceedings against the ISP. Pls.' FOF ¶ 25, Pls.' Ex. 13 (July 9, 2002 e-mail from Burfete to Ryan), Tr. 1/8/04 (Burfete) pp. 45-47.

E. ISP COMPLIANCE WITH COURT ORDERS OR INFORMAL NOTICES

1. Description of ISPs

102. AOL is an ISP located in Virginia. AOL provides, inter alia, dial-up, digital subscriber line ("DSL"), and broadband Internet access to its customers. The physical network used to provide access for dial-up and broadband customers is generally not owned or managed by AOL. Dep. of B. Patterson at 8-9, 23. AOL attorney Christopher Bubb, an assistant general counsel in AOL's legal department, testified on behalf of AOL. Dep. of C. Bubb at 10. Brooke Patterson, an employee in AOL's network operations department, also testified. Dep. of B. Patterson at 5.

103. Comcast IP Services ("Comcast") is an ISP that provides broadband Internet access to home and business subscribers and web hosting services. Dep. of G. Lipscomb at 7-8. Gary Lipscomb, the senior manager of network abuse and policy observance for Comcast, testified on behalf of Comcast. Dep. of G. Lipscomb at 5.

104. Epix Internet Services ("Epix") is a division of Commonwealth Telephone Enterprises and is based in Dallas, Pennsylvania. Epix provides dial-up and DSL Internet access, e-mail services,

and web hosting services for its customers. Epix's customers are primarily residential consumers but it also has approximately 350 commercial customers. Dep. of G. Basham at 4-8. Both Susan Butchko-Krisa, an employee in Commonwealth Telephone's legal department, and Gary Basham, a systems engineering manager for Epix, testified on behalf of Epix. Dep. of G. Basham at 5, Dep. of S. Butchko-Krisa at 15.

105. Pennsylvania Online, an ISP, provides – in central Pennsylvania – dial-up access to approximately 12,500 primarily residential customers and web hosting services to approximately 3,000 customers. Pls.' FOF ¶ 99; Tr. 1/27/04 (MacDonald) pp.126, 139-40. Michael MacDonald, who testified in this case, is the most senior technical staff member at Pennsylvania Online and is charge of running the company's network. Tr. 1/27/04 (MacDonald) at 126.

106. Verizon Internet Services ("Verizon") is an ISP that provides, inter alia, dial-up, broadband, and DSL Internet access to its customers. Dep. of R. Heister at 7-8. Richard Heister is the manager of the IP system operation for Verizon and the employees he manages are responsible for management of Verizon's DNS servers. Dep. of R. Heister at 7-8. Scott Lebredo is the senior technology manager for operations at Verizon and is primarily responsible for network security. Dep. of S. Lebredo at 10. Both of these individuals testified on behalf of Verizon.

107. WorldCom, one of the largest ISPs in the world, offers Internet access service that ranges in speed from dial-up access (about 56,000 bits per second) to more than 40,000 times that speed ("OC48" speed, about 2.5 billion bits per second) in dozens of countries around the world. WorldCom offers individual customers a choice of access methods, including dial-up and ISDN connections, as well as DSL access. Corporate and organizational customers are offered a choice of access methods including T1, frame relay, ATM, or SONET technology. Pls.' FOF ¶ 100; Tr.

1/27/04 (Krause) pp. 11, 27-28, 39-40, 42-43, 59, 61. Craig Silliman, the Director of WorldCom's Technology and Network Legal Team, and Mark Krause, the Senior Manager of Internet Infrastructure Security for WorldCom, both testified on behalf of WorldCom. Dep. of C. Silliman at 10; Tr. 1/27/04 (Krause) at 9.

2. Methods of Implementation

108. According to the ISPs, on most occasions, they attempted to comply with the Informal Notices by implementing either IP filtering or DNS filtering. These methods were either used alone or together. Jt. Stip. ¶ 51.

109. Use of IP filtering, DNS filtering, or URL filtering to block content accessible through the service of an ISP only affects Internet users who access the Internet through that ISP's service. Thus, Internet users that do not use the service of an ISP that blocked a web site would still have access to the blocked content. Tr. 1/7/04 (Clark) pp. 183-90.

a. DNS Filtering

110. "DNS filtering" is sometimes referred to as "DNS spoiling" and "DNS poisoning." Jt. Stip. ¶ 52. The Court will use the term DNS filtering to refer to this method of filtering.

111. To perform DNS filtering, an ISP makes entries in the DNS servers under its control that prevent requests to those servers for a specific web site's fully qualified domain name (found in the requested site's URL) from resolving to the web site's correct IP address. The entries cause the DNS servers to answer the requests for the IP addresses for such domain names with either incorrect addresses or error messages. Without the correct IP addresses of the requested sites, the requests either do not proceed at all or do not reach the desired sites. Joint Stip. ¶¶ 52, 53; Tr. 1/29/04 (Stern) pp. 43-45; Tr. 2/18/04 (Stern) pp. 99-100. Def.'s FOF ¶ 63.

b. IP Filtering

112. IP filtering is also referred to as null routing. Jt. Stip. ¶ 54. The Court will refer to this method as IP filtering.

113. To implement IP filtering, an ISP first determines the IP address to which a specific URL resolves. It then makes entries in routing equipment that it controls that will stop all outgoing requests for the specific IP address. Jt. Stip. ¶ 55.

c. URL Filtering

114. Mr. Stern testified that ISPs could comply with blocking orders using URL filtering. This technique was also one of the methods mentioned by Dennis Guzy, Jr. at the April 2002 meetings with ISPs. Pls.' FOF ¶ 435; Tr. 1/12/04 (Guzy, Jr.) pp. 16-17. URL filtering involves the placement of an additional device, or in some cases the reconfiguration of an existing "router" or other device, in the ISP's network to (a) reassemble the packets for Internet traffic flowing through its network, (b) read each http web request, and (c) if the requested URL in the web request matches one of the URLs specified in a blocking order, discard or otherwise block the http request. Tr. 1/7/04 (Marcus) pp. 34-35; Tr. 2/26/04 (Marcus) p. 6; Pls.' FOF ¶ 436.

3. <u>Comparison of Filtering Methods</u>

a. Ease of Implementation and Cost

115. The ISP market is very competitive and the speed and performance of a network is an important factor in the public's perception of an ISP. Tr. 2/18/04 (Stern) p. 77. Because the market for Internet access is "very competitive," if an ISP were to implement a [filtering method] which adversely affected [its] network performance . . . [or] if [its] network became slower, it would be added incentive for [its] customers to jump ship." Pls.' FOF ¶ 102; Tr. 1/27/04

(MacDonald) pp. 136-38.

116. Most ISPs already have the hardware needed to implement IP filtering and IP filtering is a fairly routine aspect of the management of a network. IP filtering is used to respond to various types of attacks on a network, such as denial of service attacks and spam messages. Pls.' FOF ¶ 237; Tr. 3/1/04 (Blaze) pp.14-15 (explaining denial of services attacks and spam); Tr. 1/7/04 (Marcus) p. 55. For example, IP null routing (or IP filtering) is something that WorldCom uses "routinely." Pls.' FOF ¶ 237; Tr. 1/27/04 (Krause) pp. 78-80. WorldCom has an automatic system (developed for network management reasons unrelated to Pennsylvania blocking orders) that can implement an IP null route on all of WorldCom's thousands of routers "relatively instantaneously, within a matter of seconds to minutes." Pls.' FOF ¶ 238; Tr. 1/27/04 (Krause) p.52. For AOL, IP filtering is "in common use as a defensive mechanism against such activities as virus proliferation, spam, et cetera. It is a basic and common tool of the trade." Dep. of B. Patterson (AOL) at 38.

117. IP filtering generally does not require ISPs to purchase any new equipment and it does not have any impact on network performance. Pls.' FOF ¶ 239; Dep. of B. Patterson (Senior Network Administrator for AOL) at 38-40, 52. Dennis Guzy, Jr., testified that IP filtering is "easy to perform" and is indeed the "easiest" method of filtering for an ISP to use. Pls.' FOF ¶ 237; Tr. 1/12/04 (Guzy Jr.) pp. 76-77; Pls.' Ex. 85 (Nov. 18, 2002 memo by Dennis Guzy, Jr.). Most ISPs can implement IP filtering with their existing equipment and many ISPs already have an existing internal procedure to implement IP-based blockage. Tr. 2/18/04 (Stern) pp. 23-24.

118. Most ISPs that do not outsource Internet access would not be required to purchase new equipment to implement DNS filtering. If the ISP's staff is familiar with this method of filtering, the necessary entries in the DNS servers require no expenditure of money and little staff time. Tr.

1/29/04 (Stern) pp. 87-93; Tr. 1/7/04 (Marcus) pp. 17-24; Hiester Dep. pp. 33-35, 45-47; Basham Dep. pp. 16, 73. Almost all ISPs that do not outsource Internet access can utilize DNS filtering for customers that use their DNS servers. Tr. 1/29/04 pp. 67 (Stern); Tr. 1/27/04 (Krause) pp. 68-70; Tr. 1/27/04 (MacDonald) pp. 147-148, 159; Patterson Dep. pp. 15-16, 123-125, 131; Def.'s FOF ¶ 74.

119. DNS filtering would be more difficult for some ISPs to implement. Compared to IP filtering, as Professor Blaze explained, DNS filtering is a "much more specialized technique" within the network security field. Tr. 3/1/04 (Blaze) pp. 15-16. According to Mark Krause of WorldCom, DNS filtering is "not a very standard process" and "not something that ISP[s] would normally do." Pls.' FOF ¶ 241; Tr. 1/27/04 (Krause) p. 75.

120. AOL does not currently perform DNS filtering on its network. As of February 3, 2004, AOL would have been required to make entries manually in all of its 100 DNS servers to implement a DNS block. Automating this process would involve designing a new system to do DNS filtering, assessing the related risks, assigning additional long-term staff, and developing auditing and monitoring systems. Dep. of B. Patterson at 47-51, 136-42. Given these factors, Mr. Patterson said he would recommend IP filtering to AOL; he would not recommend DNS filtering. Id. at 51-52.

121. DNS filtering would "require [WorldCom] to radically redo the way [it] currently implement[s] [its] DNS system to [its] customers." Tr. 1/27/04 (Krause) pp.16-17. WorldCom does not have "a built-in infrastructure to push out configuration changes to those [DNS] systems" (Id. at 17) and implementing DNS filtering would require WorldCom to purchase and configure additional DNS servers in its network and potentially reconfigure the systems of

millions of customers. Id. at 17-18.

122. With the exception of AOL and WorldCom and other ISPs that do not currently perform DNS filtering, the cost of implementing IP filtering and DNS filtering is "approximately equal." Tr. 1/29/04 (Stern) p.128. More generally, the difficulty of implementation, financial cost, and performance impact of DNS filtering and IP filtering are similar. Pls.' FOF ¶ 245; Tr. 2/18/04 (Stern) pp. 46-47.

123. No ISPs known to either plaintiffs' or defendant's experts utilize URL filtering to screen all World Wide Web traffic. Tr. 1/6/04 (Marcus) pp. 130; Tr. 1/29/04 (Stern) pp. 20-22; Tr. 1/7/04 (Smallacombe) p. 84; Dep. of C. Silliman (WorldCom) at 166; Dep. of G. Basham (Epix) at 27-28. AOL performs URL filtering on a portion of its network, but it cannot utilize URL filtering on its entire network at the present time. AOL calls this URL filtering service "parental controls." AOL engineer Patterson explained that to undertake URL filtering for all AOL members would require expenditures for development, installation, new hardware and software, management costs, performance assessments, customer support, and further re-engineering of the network. It would take years to implement and be "extraordinarily expensive." Dep. of B. Patterson (AOL) at 60-63, 66-67, 75-76, 181-87; Pls.' FOF ¶ 449; Dep. of C. Bubb (AOL) at 129, 173-75; Pls.' FOF ¶ 452. AOL's parental controls are engineered, architected, and scaled to handle only a certain percentage of AOL's traffic; these controls could not perform filtering for all AOL member traffic. Dep. of B. Patterson (AOL) at 60-63.

124. ISPs would be required to develop new equipment and conduct testing with this equipment before implementing URL filtering. For example, an ISP would be required to purchase substantially more switches and routers to maintain the network's prior level of capacity because

the switches and routers can handle less traffic if they are performing the computations necessary for URL filtering. Tr. 2/26/04 (Marcus) pp. 5-7, 45-48; Pls.' FOF ¶ 445. Mr. Stern acknowledged that any implementation of URL filtering would require extensive research and testing, and he admitted that he had not done such testing and did not know of anyone who had done so. Tr. 1/29/04 (Stern) pp. 20-22; Tr. 2/18/04 (Stern) pp. 67-68. Mr. Stern also admitted that most ISPs do not have the hardware or software required to implement URL filtering. Tr. 2/18/04 (Stern) pp. 69-72; Pls.' FOF ¶¶ 438.

125. If an ISP did not purchase substantially more switches and routers, URL filtering would "significantly degrade" the performance of an ISP's network. Tr. 1/6/04 (Marcus) p.123; Tr. 2/18/04 (Stern) pp. 72-75. Such degradation is caused by the fact that the technical process of comparing all of the URLs in the web traffic flowing through an ISP's network with a list of URLs to be blocked is "expensive" in the computational sense – it requires a significant amount of computing power. Performing these computations would slow down each switch and router substantially and descrease the overall capacity of the network. Tr. 1/6/04 (Marcus) pp.122-27; Tr. 2/26/04 (Marcus) pp. 5-6, 32, 50-51 (M.Marcus); Pls.' FOF ¶ 441.

126. The purchase and testing of the equipment necessary to perform URL filtering would require a significant investment by ISPs. Engineers from Epix, Verizon, Pennsylvania Online, Plantagenet, and WorldCom all testified that their ISPs do not perform any URL filtering. Dep. of G. Basham (Epix) at 27-28; Dep. of R. Hiester (Verizon) at 81-83; Tr. 1/27/04 (MacDonald – Pennsylvania Online) p. 133; Tr. 1/7/04 (Smallacombe – PlantageNet) pp. 95-96; Tr. 1/27/04 (Krause – WorldCom) p. 20. It would cost Verizon "well into seven figures" to implement URL filtering across its entire network. Dep. of R. Hiester (Verizon) at 83. "[M]oney aside, the

current [URL filtering] technology . . . would not be able to even operate in [WorldCom's] network" because the current URL filtering products (a) cannot support the speeds needed in WorldCom's network and (b) do not connect to the type of physical wiring (such as fiber optic and coaxial copper cable) that WorldCom uses. Tr. 1/27/04 (Krause) p. 21-22, 87-89.

b. Relative Effectiveness

127. An ISP's use of DNS filtering does not impact customers that do not use the ISP's DNS servers. Pls.' FOF ¶ 247; Tr. 1/6/04 (Marcus) pp. 115-18; Tr. 2/18/04 (Stern) p. 47. Customers are not required to use the DNS server provided by their ISP. Mr. Stern specifically acknowledged that "[l]arge businesses often operate their own [DNS servers]." Pls.' FOF ¶ 248; Tr. 1/29/04 (Stern) pp. 68-69.

128. Because DNS filtering is not effective for all of their customers, some ISPs chose not to use this method.

(a) Pennsylvania Online does not require its customers to use its DNS servers and does not know whether any particular customer uses its DNS servers. Tr. 1/27/04 (MacDonald) pp. 145-48. Pennsylvania Online used IP filtering to comply with the Informal Notices it received because it was the "most effective solution to [e]nsure compliance" and because DNS filtering can be "easily circumvent[ed]" by customers running their own domain name server. Id. at 131-32; Pls.' FOF ¶ 250.

(b) WorldCom did not use DNS filtering for two reasons. First, WorldCom could not easily implement this method for the reasons set forth in Finding of Fact 121. Second, "[DNS filtering] would not allow [WorldCom] to fully comply with the court order . . . due to the fact that not all of [WorldCom's] users use DNS servers under its control." Tr. 1/27/04 (Krause) p.

16. According to Mr. Krause, medium and large businesses often operate their own DNS servers. Id. at 76-77; Pls.' FOF ¶ 251. WorldCom's customer base is primarily businesses and ISPs (to whom WorldCom provides wholesale Internet access) that maintain their own DNS servers. Thus, in terms of compliance with a court order, WorldCom "thought that [DNS filtering] simply was so seriously flawed that it was not a workable solution." Mr. Silliman expressed these concerns to the OAG. Pls.' FOF ¶ 252; Dep. of C. Silliman (WorldCom) at 104-06, 110-11, 133.

(c) AOL was concerned that the 67 district attorneys empowered to enforce the Act might not agree with the OAG's opinion that DNS filtering was an acceptable method of compliance. Dep. of C. Bubb (AOL) at 207-08. Furthermore, AOL's users could change their configurations to different DNS servers either manually or by loading applications that do it for them. Additionally, some customers that access AOL using a broadband Internet connection are assigned a different DNS server by the third party providing the broadband service. Dep. of Patterson at 16, 44-45.

129. Other ISPs informed the OAG they were concerned about the use of DNS filtering because they had customers that did not use their DNS servers and would be unaffected by such filtering. For example, Verizon informed the OAG that not all of its customers used its DNS servers, and DNS filtering for those customers would not be effective. Pls.' FOF ¶ 254; Tr. 1/9/04 (Guzy Sr.) p. 160-61; Pls.' Ex. 84 (Aug. 16, 2002 letter from Verizon to OAG); Dep. of S. Lebredo (Verizon) at 25. Moreover, the Attorney General was on notice of this problem with DNS filtering because the OAG operates its own DNS server. The approximately 1,000 employees of the OAG do not rely on the DNS server of the OAG's ISP, Verizon, and would not be affected by Verizon's use of DNS filtering. Pls.' FOF ¶ 255; Tr. 1/12/04 (Guzy Jr.) p. 72.

130. Some small entities do not use the DNS server of their ISP. For example, CDT does not use the DNS server of its ISP. In early 2000, Mr. Clark decided that the performance of its ISP's DNS servers was unacceptable, and he set up the CDT system use its web host's DNS servers. Pls.' FOF ¶ 257; Tr. 1/28/04 (Clark) p. 75.

131. Even a home user can redirect his computer to a DNS server not controlled by his ISP. However, redirection is not something home users who are not actively seeking child pornography are likely to do to any great degree. It requires knowledge that it is possible, an understanding of how to accomplish it, knowledge of the IP address of an alternate DNS server, and knowledge of the steps, often complicated, that must be taken to enter that IP address into the user's computer. Tr. 1/29/04 (Stern) pp. 80-83; Tr. 1/7/04 (Marcus) pp. 26-29; Tr. 1/7/04 (Smallacombe) pp. 113; Lebredo Dep. pp. 118-119; Hiester Dep. pp. 38-39.

132. Mr. Stern opined that employees of ISPs' corporate customers that operate their own DNS servers would not be able to access child pornography because some of these corporations operate filtering products that limit their employees' access to objectionable content. Tr. 1/29/04 (Stern) pp.75-77. However, not all corporations use corporate filtering products, and an ISP cannot reliably or easily determine whether its customers use corporate filtering. Tr. 1/7/04 (Marcus) pp. 47-48, Tr. 2/18/04 (Stern) pp. 48-50. As a result, an ISP cannot rely on corporate filtering to block access for customers who do not use DNS servers under its control.

133. IP filtering would be effective even where a user did not rely on the ISP's DNS server. Pls.' FOF ¶ 263; Tr. 2/18/04 (Stern) p.36.

134. A child pornography web site can evade an IP filter by obtaining a new IP address for the web site. Tr. 1/7/04 (Marcus) pp. 14-15. A web site's IP address can change without the

URL changing. Tr. 1/29/04 (Stern) pp. 62-63, 65. If, however, the ISP implementing the IP filter monitors the web site for a new IP address and changes the IP address being filtered to block the new address, the IP filtering is still effective. Id. at 15. Such a monitoring program is easy to create. Pls.' FOF ¶ 261; Tr. 2/18/04 (Stern) pp. 33-34. WorldCom utilized IP filtering monitors – it "implemented a tool to monitor for any of those [IP address] changes and to alert [WorldCom] to [the change], so that then [it] could go and adjust the null routing to follow the change made in the DNS." Pls.' FOF ¶ 262; Tr. 1/27/04 (Krause) p. 80.

135. Because DNS filtering stops a request for the domain name before it has been resolved to an IP address, it continues to prevent access to the identified child pornography item even if the offending site changes its IP address. Tr. 1/29/04 (Stern) pp. 62-64; Tr. 2/18/04 (Stern) p. 136; Tr. 1/7/04 (Marcus) pp. 18-19; Def.'s FOF ¶ 65.

136. IP filtering is more effective than DNS filtering because IP filtering blocks content for all users, including those who do not use DNS servers under an ISP's control. Although a web host can evade IP filtering by changing a web site's IP address – a technique that will not defeat DNS filtering – an ISP can track these changes and block the new IP address. Pls.' FOF ¶ 260; Tr. 1/29/04 (Stern) pp. 127-28; Tr. 1/7/04 (Marcus) pp. 49-50; Tr. 2/18/04 (Stern) pp. 31-32. Thus, it is reasonable for an ISP to chose IP filtering as a method of compliance over DNS filtering.

c. Overblocking

137. DNS filtering stops requests for all sub-pages under the blocked domain name. Thus, if the domain name included in the URL identified by an Informal Notice is of a Web Hosting Service that allows users to post their independent content as sub-pages on the service's site, the DNS server entries will stop requests for all of the independent pages on the service, not just the page

that displays the targeted child pornography item. Tr. 1/29/04 (Stern) pp. 50-51; Tr. 2/18/04 (Stern) pp. 103-107. For example, DNS filtering results in overblocking when an online community such as the GeoCities web site, which allows many different users to have web sites on sub-pages of GeoCities.com, is targeted by an Informal Notice. Pls.' FOF ¶ 285; Tr. 1/6/04 (Marcus) pp. 109-10; Tr. 2/18/04 (Stern) pp. 54-56, 60.

138. DNS filtering stops requests for the domain name, not the IP address for the domain name; it does not disable access to any domain names that share an IP address with the targeted site unless they also share a domain name. Tr. 1/29/04 (Stern) pp. 61-62; Tr. 1/7/04 (Marcus) p. 18; Hiester Dep. pp. 35-36; Basham Dep. p. 23.

139. DNS filtering stops requests only for the domain name specified, it does not stop requests for parent domains or sibling sub-domains of the domain name. Thus, if the filtering stops requests for subdomaina.da.ru, it will not stop requests for da.ru or subdomainb.da.ru. Tr. 1/29/04 (Stern) pp. 45-49, 54-62; Tr. 2/18/04 (Stern) pp. 57-59, 107; Tr. 1/7/04 (Marcus) pp.18-19; Def.'s FOF ¶¶ 69-70. However, if the parent domain is filtered, requests for sub-domains would be blocked. Thus, if da.ru was blocked, subdomaina.da.ru and subdomainb.da.ru would also be blocked. Tr. 2/18/04 (Stern) p. 54.

140. IP filtering leads to a significant amount of overblocking. As Mr. Stern stated, IP filtering "will block innocent sites to a great deal," Tr. 1/29/04 (Stern) p. 65, and "IP address filtering is extremely likely to block untargeted sites due to the process known as virtual hosting," Id. at 128. Dennis Guzy Jr. reached an identical conclusion, stating that it is "very easy to block access to additional sites" when using the IP filtering method. Pls.' FOF ¶ 282; Pls.' Ex. 85 (Nov. 18, 2002 memo from Guzy, Jr.).

141. IP filtering leads to blocking, of innocent web sites, because of the prevalence of shared IP addresses, as detailed in Findings of Fact 16, 42, and 43. If an ISP uses IP filtering to block access to a particular IP address, all web sites hosted at that IP address are blocked. Tr. 1/6/04 (Marcus) pp. 103-04. As an example, in response to Informal Notice 2545, Epix.net blocked access to IP address 204.251.10.203, which in turn blocked access to two of Laura Blain's web sites and others hosted by directNIC. Pls.' FOF ¶ 283; Pls.' Ex. 54 (Informal Notice 2545); Pls.' Ex. 56 (internal Epix.net e-mail indicating that 204.251.10.203 blocked in response to Informal Notice 2545 and that this was also the IP Address for directnic.com's hosting service).

142. URL filtering filters out URLs down to the specific subpage. It presents no risk of disabling access to untargeted sites. Tr. 1/29/04 (Stern) p. 102; Tr. 2/18/04 (Stern) p. 106; Tr. 1/6/04 (Marcus) p. 122; Def.'s FOF ¶ 112.

143. Although URL filtering results in the least amount of overblocking, no ISPs are currently capable of implementing this method. Both DNS filtering and IP filtering result in overblocking.

4. <u>Contacting the Host</u>

144. Although not a technical method of compliance, there is evidence that both ISPs and the OAG have located and contacted the hosts of web sites alleged to contain child pornography and asked the hosts to remove the sites from their services or servers. Jt. Stip. ¶ 56. If alleged child pornography resides on the service of an ISP – as contemplated by the Act – the ISP would use the same method to remove the web site from its service or server.

145. Entities that host web sites can easily remove sites, or content, residing on their Web Servers. Tr. 1/28/04 (Clark) p. 151; Tr. 1/9/04 (Guzy Jr.) p. 86; Silliman Dep. pp. 18-19; Bubb Dep. pp. 17, 159-162. This action removes the content from the Internet but affects no other site

or content, other than that removed. Tr. 1/29/04 (Stern) p. 52; Def.'s FOF ¶ 52-54; Tr. 1/8/04 (Burfete) pp. 39-40; Tr. 2/18/04 (Stern) pp. 90-91.

146. A number of ISPs do not view contacting the host as an acceptable method of compliance with the Act. Epix never considered contacting a web host and asking it to remove illegal content. Dep. of G. Basham (Epix) at 28-29. AOL did not view contacting the web host as a viable method of compliance because of the risk of liability. AOL did not want its "criminal liability rest[ing] on the actions of a third party over which [it] had no control." Dep. of C.Bubb (AOL) at 190-91. Aside from a Web Hosting Service, Comcast did not considered contacting the host as a compliance option. Gary Lipscomb opined that Comcast had to comply with the Informal Notice by taking action that was within its control. Dep. of G.Lipscomb (Comcast) at 45-46.

147. The "contacting the host" method of compliance is not mentioned in the Act, and OAG's current position that contacting the host constitutes compliance is not binding on either future Attorneys General or current or future county district attorneys. Tr. 1/9/04 (Burfete) pp. 20-22.

148. Web Hosting Services that host web sites as sub-pages under their domains usually remove pages where child pornography resides once they learn of it. Tr. 1/9/04 (Guzy Sr.) p. 86; Tr. 1/12/04 (Guzy Jr.) pp. 30-31; Tr. 1/29/04 (Stern) pp. 51, 52; Tr. 2/18/04 (Stern) pp. 103-105, 137; Tr. 1/7/04 (Marcus) p. 22; Lebredo Dep. pp. 57-59, 115-118.

149. For those ISPs that contacted the web host, that contact generally resulted in removal of the alleged child pornography from the Internet. For example, Mr. Lebredo of Verizon stated that he had never contacted a hosting company that refused to remove child pornography – "[b]ased on five years of working closely with law enforcement in the . . . Internet community, I've never

come across a non-cooperative entity when it came to child pornography." Dep. of S. Lebredo (Verizon) at 92. Similarly, Mr. Silliman of WorldCom explained that the task of contacting a web hosting company is easy to undertake and appears to be effective most of the time. Dep. of C. Silliman (WorldCom) at 78-90. Likewise, Comcast explained that it had contacted the web host on two or three occasions when it was concerned that instituting a block would also block innocent web sites and that such contacts were successful. Dep. of G. Lipscomb (Comcast) at 37-38; Pls.' FOF ¶ 554.

150. The OAG prepared statements of recommended language for telephone contact with Web Hosting Services to request that they remove posted child pornography. Pls.' Exs. 39 ("Recommended language for telephone contact with Web Hosting Services in lieu of Informal Notice" script), 40 ("Amended Recommended language for telephone contact with Web Hosting Services in lieu of Informal Notice" script); Tr. 1/8/04 (Burfete) pp. 95-97. When investigators were given information about a Web Hosting Service that hosted child pornography, they contacted the host and asked it to remove the offending materials from its service. In every instance, the hosting entity promptly complied with the request. According to Agent Guzy, "[t]hey always comply." Tr. 1/9/04 (Guzy Sr.) pp. 85-86, 149-50; Tr. 1/8/04 (Burfete) pp. 82-84; Pls.' FOF ¶ 555. The OAG contacted the web host in more than 70 cases involving Web Hosting Services. All such contacts resulted in removal of the designated child pornography from the Web Hosting Service.

151. The information needed to track down the entity to which an IP address has been assigned is publicly available, and ISPs have no greater access to this information than the OAG. Tr. 1/27/04 (Krause) pp.109-11. There are a number of software tools available on the Internet

that provide information about the entity to which an IP address has been assigned from the registries responsible for assigning IP addresses. Tr. 1/12/04 (Guzy Jr.) pp. 57-61; Tr. 1/28/04 (Clark) pp. 68-69. It takes only a few minutes to track down the appropriate contact for a web hosting company. Dep. of G. Lipscomb (Comcast) at 104-05; Dep. of C. Silliman (WorldCom) at 80; Dep. of S. Lebredo (Verizon) at 94.

152. Dennis Guzy Jr. was able to locate the individual responsible for a Web Hosting Service in all instances in which he tried to do so. Id. at 31, 36-37. The OAG's experience in trying to locate appropriate contact persons demonstrates that such investigation is within the competency of the OAG staff. Tr. 1/12/04 (Guzy Jr.) pp.57-61.

153. In practice, the OAG has accepted contacting the host as a method of compliance. For example, in June 2002, AOL called Mr. Burfete and told him that the operator of a Web Hosting Service had removed a child pornography item referenced by an Informal Notice from its service, and AOL then lifted its block on the service. Mr. Burfete informed AOL that he approved of its action. Bubb Dep. pp. 60-65; Tr. 1/8/04 (Burfete) pp. 64, 135. In addition, the OAG informed WorldCom that contacting the host was an acceptable method of compliance with the court order issued to WorldCom. Jt. Ex. 5 (Sep. 17, 2002 letter from Burfete to Silliman).

154. Even if law enforcement or an ISP can identify the site's immediate host, it may be in a foreign country. Foreign hosts, outside the reach of United States laws, may not be as willing to remove sites from their services as domestic hosts. Tr. 1/12/04 (Guzy Jr.) pp. 122-123; Lebredo Dep. p. 118; Silliman Dep. pp. 85-89, 152-156.

155. If an ISP cannot contact the host or the host is not willing to comply, the ISP would be required to implement a filtering method to deny access to the site. For example, WorldCom

attempted to contact the host for all five URLs identified in the court order it received. For two of these sites, WorldCom was not able to verify that the web host had removed the offending content, and it implemented IP filtering to disable access to these URLs. Jt. Ex. 8 (Sep. 23, 2002 letter from Silliman to Burfete).

156. Of all the methods used by ISPs to comply with Informal Notices or court orders – IP filtering, DNS filtering, and contacting the host – contacting the host results in the least amount of overblocking. However, it is not a complete solution because there is evidence that an ISP or the OAG cannot always contact a web host and a web host will not comply in every instance. If an ISP cannot contact the host or is unwilling to rely on the actions of a web host, it must implement a filtering method to comply with an Informal Notice or court order.

5. <u>Specific Examples of ISP Compliance</u>

157. The parties compiled a list of "all or almost all" Informal Notices sent by the Attorney General to ISPs, excluding notices sent directly to Web Hosting Services. This list was received in evidence as Joint Exhibit 9. Joint Exhibit 9 lists "the ISP that received the Informal Notice, the actual or approximate date of the Notice, the Notice Number (if known), the URL specified in the Notice, the technical action by the ISP in response to the Notice (if known), and the IP address blocked by the ISP (where applicable and if known)." Jt. Stip. ¶ 60. The contents of Joint Exhibit 9 are summarized as follows:

a. AOL received 123 notices. AOL used IP Filtering to disable access to the URL in 78 cases. For most of the remaining URLs, AOL's response is either unknown or AOL took no action because the URL was either not found or invalid. In two instances, Notices 4918 and 9489, AOL contacted the OAG because it did not want to block access to

www.terra.es and www.trafficgizmo.com, large online communities. AOL informed the OAG that blocking access to these communities would block hundreds of thousands of untargeted web sites, and the OAG did not require AOL to block access to these sites. Jt. Stip. ¶ 60(b)(1), Pls.' Ex. 46 (AOL's Response to Oct. 22, 2003 subpoena). C. Bubb. Dep. at 60-62, 137

b. Comcast received 126 notices. Comcast used IP filtering to disable access to the URL in 125 cases. In one case, Notice 1757, Comcast contacted the web host. Jt. Stip. ¶ 60(b)(2).

c. CompuServe received 7 notices and used IP filtering to disable access in all 7 cases.

d. Eathlink received 56 notices and used DNS filtering to disable access in all 56 cases. Jt. Stip. ¶ 60(b)(3).

e. Epix received 48 notices. Epix used both IP filtering and DNS filtering to disable access in 18 cases and DNS filtering alone in the remaining 30 cases. Jt. Stip. ¶ 60(b)(4).

f. Erols.com received one Informal Notice that was withdrawn by the OAG. Jt. Stip. ¶ 60(b)(5).

g. Innernet.net received 4 Informal Notices and used IP filtering to disable access in all cases. Jt. Stip. ¶ 60(b)(7).

h. Pennsylvania Online received 2 Informal Notices and used IP filtering to disable access in both cases. Jt. Stip. ¶ 60(b)(10).

i. RCN Internet received 4 notices. RCN used DNS filtering to disable access in one case, DNS filtering and IP filtering in one instance; and its actions in the remaining two cases are unknown. Jt. Stip. ¶ 60(b)(12).

j. Verizon received 112 notices. Verizon used DNS filtering in response to 7 notices and DNS filtering and IP filtering in response to 104 notices. In one case, the informal notice was sent to Verizon in error, and Verizon forwarded the notice to GeoCities. In some cases, blocking was implemented by Verizon's third party network providers. Jt. Stip. ¶ 60(b)(14).

k. WorldCom received 10 notices. WorldCom did not take any action in response to the Informal Notices. Jt. Stip. ¶ 60(b)(15).

l. For the following ISPs, the actions taken in response to Informal Notices are unknown:

i. FYI Networks (1 notice). Jt. Stip. ¶ 60(b)(6).

ii. Microsoft (6 notices). Jt. Stip. ¶ 60(b)(8).

iii. NFDC (1 notice). Jt. Stip. ¶ 60(b)(9).

iv. PennTeleData (2 notices). Jt. Stip. ¶ 60(b)(11).

v. Superpa (2 notices). Jt. Stip. ¶ 60(b)(13).

158. WorldCom implemented IP filtering in response to a court order for the two web sites whose host it was not able to contact. WorldCom's decision to use IP filtering instead of DNS filtering was based "primarily" on the fact that DNS filtering would be ineffective for WorldCom's customers that did not use WorldCom's DNS servers, and IP filtering was easier for WorldCom to implement than DNS filtering. Pls.' FOF ¶ 268; Tr. 1/27/04 (Krause) pp. 16-17.

159. A number of ISPs chose not use DNS filtering because DNS filtering is not effective for customers that do not use DNS servers under its control. FOF ¶ 128.

160. When Comcast received its first Informal Notice, it attempted to apply a block at Comcast DNS servers. Dep. of G. Lipscomb (Senior Manager of Network Abuse and Policy Observance

for Comcast) at 18. It took three days for that change to propagate to all of the DNS servers in the Comcast network, and with only five days to comply with an Informal Notice, Comcast concluded that implementation of DNS filtering was too slow. Id. at 21. As a result, Comcast chose to use IP filtering as its method of compliance "because it was most effective." Id. at 26.

161. At least 27 of the Informal Notices specified IP addresses instead of URLs. Jt. Exh. 9 (Agreed Lists of Informal Notices), Tab B, lines 2-9, 121-22, 125-41. If an ISP received a blocking order containing an IP address, it could not use DNS filtering to comply with the order. A user's request for an IP address is not resolved by a DNS server and, as a result, the request does not travel through the domain name system. Pls.' FOF ¶ 271; Tr. 1/7/04 (Marcus) pp. 41-42.

162. It is the official position of the OAG to refuse to tell an ISP whether any particular method of filtering complies with the law. Pls.' FOF ¶ 273; Tr. 1/8/04 (Burfete) pp. 133-35; Tr. 1/9/04 (Guzy Sr.) p. 178.

163. The OAG never objected when ISPs advised the office that they were using DNS filtering to comply with an Informal Notice. Tr. 1/9/04 (Guzy Sr.) pp. 134-136; Tr. 1/12/04 (Guzy Jr.) p. 27; Def.'s Ex. 12 (May 1, 2002 letter from Verizon to OAG); Pls.' Ex. 23 (May 1, 2002 e-mail from Guzy to CSEU); Basham Dep. pp. 19-23, 57-60; Butchko-Krisa Dep. pp. 11-14, 19-22; Tr. 1/8/04 (Burfete) pp. 133-134.

6. Blocking of Innocent Web Sites

164. Mr. Clark created a database to measure the prevalence of shared IP addresses. The parties stipulated that, for a number of reasons, his database is a "rough approximation" of the extent of IP address sharing. Jt. Stip. ¶ 59; Finding 44. As a result, when the Court refers to a specific number of innocent sites that were blocked by an ISP, this number is also an approximation.

Although not exact, the numbers reflect the magnitude of overblocking that resulted from ISP compliance with the Act.

a. Laura Blain

165. Laura Blain served as the webmaster for a number of community organizations in rural Pennsylvania, including the Sheshequin-Ulster Community Center. Ms Blain created a web site for the community center in February 2003 in part to share information with township officials who controlled funding for the center. Tr. 1/6/04 (Blain) pp. 26, 28. The web site, located at http://www.sheshequinulsterreccenter.org/, contains, for example, minutes of board meetings, news articles, information on ice skating programs and other information related to the community center. Id. at 26-28; Pls.' Exh. 104, Tab 8 (screen shots from http://www.sheshequinulsterreccenter.org/); Pls.' FOF ¶ 290.

166. Ms. Blain chose directNIC as the web hosting service for her community center because this company offered her free hosting space in exchange for putting a small banner advertisement for their service on her web site. Pls.' FOF ¶ 96, Tr. 1/6/04 (Blain) pp. 26-30 (describing creation of free and low-cost web sites for two community organizations).

167. Ms. Blain also created a web site for the Pennsylvania Hinterland Cyber Charter School based in Ulster, Pennsylvania. Tr. 1/6/04 (Blain) pp. 28-30; Pls.' Ex. 55 (screen shot from http://pahinterlandschool.org). Again she chose to use the directNIC web hosting service, but she opted for an advertisement-free web site for the school and paid a fee to directNIC to host the web site. Tr. 1/6/04 (Blain) p. 29; Pls.' FOF ¶ 292.

168. To gain access to the Internet, Ms. Blain used the services of a local Pennsylvania ISP, Epix, which provided her with high-speed DSL service at her home and dial-up service at her

office. Tr. 1/6/04 (Blain) p. 24.

169. On July 1, 2003, the OAG issued Informal Notice 2545 to Epix, directing Epix to block access to a specified URL. Pls.' Ex. 54 (Informal Notice 2545); Jt. Ex. 9 (Agreed Lists of Informal Notices), Tab A, line 324 (listing Notice 2545).[4] As a result of that Informal Notice, Epix blocked access to IP address 204.251.10.203. Pls.' Ex. 56 (internal Epix e-mail indicating that 204.251.10.203 blocked in response to Notice 2545).

170. IP address 204.251.10.203 was the IP address that directNIC had assigned to both the community center and the school web sites operated by Ms. Blain. Pls.' Ex. 53, pp. 5, 6 (e-mail from Blain dated July 7, 2003 showing results of ping and tracert tests for Ms. Blain's web sites); Pls.' FOF ¶ 295. According to the database developed by Mr. Clark, at least 15, 574 other sites shared this IP address in October of 2003. Tr. 1/7/04 (Clark) pp. 141-42.

171. In early July 2003, it came to Laura Blain's attention that the community center web site was not accessible to all Internet users. She confirmed that she was unable to access the web sites of the community center and the charter school through her ISP, Epix. Assuming that the problem was with her web hosting service, Ms. Blain filed a trouble ticket with directNIC on July 3, 2003, and commenced an eight-day troubleshooting process to determine why the web sites were not available. When five days of extensive testing by directNIC and Ms. Blain did not solve the problem, Ms.Blain called her ISP, Epix. Tr. 1/6/04 (Blain) pp.30-31, 42; Pls.' Ex. 53 (e-mails exchange between Blain and directNIC); Pls.' FOF ¶ 296.

172. Epix thereafter determined that the Blain web sites were hosted on an IP address that had

---

[4]Because the Court does not know whether the web site identified by this URL still contains child pornography, the Court will not identify the URL.

been blocked in response to an Informal Notice. Dep. of G. Basham (Epix) at 54-57.

173. On July 9, 2003, Mr. Basham notified Ms. Butchko-Krisa that a customer was unable to access a site that shared an IP address with a site that Epix had blocked in response to an Informal Notice. Pls.' FOF ¶ 301; Pls.' Ex. 56 (July 9, 2003 e-mail from Basham to Butchko-Krisa).

174. On July 10, 2003, Ms. Butchko-Krisa explained to Mr. Burfette that innocent web sites had been blocked as a result of the Informal Notice. He told her he was aware that IP filtering could result in the blocking of additional sites. As a result of this conversation, she decided that Epix was not required to institute IP filtering and could rely on DNS filtering alone. Tr. 1/8/04 (Burfete) pp. 68-70, 134; Pls.' Ex. 54 (Burfetes's notes of conversation his conversation with Epix); Pls.' Ex. 57 (July 10, 2003 Butchko-Krisa memorandum); Dep. of S. Butchko-Krisa (Epix) at 19-21.

175. After the conversation with Mr. Burfete on July 10, 2003, Epix utilized DNS filtering only, and it removed the blocks on IP addresses that it had instituted in response to Informal Notices. Dep. of G. Basham (Epix) at 57; Dep. of S. Butchko-Krisa (Epix) at 28-29. Ms. Butchko-Krisa testified that Epix lifted the IP address block of Ms. Blain's sites after she spoke to Special Agent Guzy on July 9, 2003, but Ms. Blain testified that she remained unable to access the sites through Epix until July 11, 2003. Tr. 1/6/04 (Blain) pp. 37-38, 40-41; Dep. of S. Butchko-Krisa (Epix) at 28; Pls.' FOF ¶ 304.

176. Because she was unable to access the web sites during this period, Ms. Blain asked directNIC to move the web sites to a different IP address, a process that took several days. Tr. 1/6/04 (Blain) pp. 37-38, 40-41. The unavailability of the community center's web site occurred soon after the center had received funding from its town government, and the web site was an

important means to communicate with the government. According to Ms. Blain, "I had gone through a year and a half of rebuilding burnt bridges with [the town govnernment] from the prior board for the Rec Center. . . . They had just on July 3rd returned our funding to us. For me to suddenly not have a web site available for them to look at could have severely burned all those bridges again." Tr. 1/6/04 (Blain) pp. 37-38. Ms. Blain concluded that the charter school could not afford to be "off-line" for the time it would take directNIC to move the web site to a new IP address. Thus, Ms. Blain was forced to purchase web hosting services for the charter school from another company. Tr. 1/6/04 (Blain) p. 38.

177. Other than Epix in July 2003, no ISP that disabled access to a site in response to an Informal Notice asked the OAG whether it could terminate its disabling action. Tr. 1/9/04 (Guzy Sr.) pp. 106-107, 146-147.

b. Evidence of Other Blocked Sites

178. On June 3, 2002, the OAG issued Informal Notice 7005 to AOL. Pls.' Ex. 47 (Informal Notice 7005); Jt. Ex. 9, Tab C, line 17 (listing Notice 7005). As a result of receiving that Informal Notice, AOL blocked access to IP address 216.148.221.150. Pls.' Ex. 46 (internal AOL spreadsheet indicating that 216.148.221.150 was blocked in order to block access to URL specified in Notice 7005) at 2, line 10. This Informal Notice led to the blocking of hundreds of thousands of web sites that shared the IP address that AOL had blocked. Tr. 1/8/04 (Burfete) pp. 63-65; Pls.' Ex. 48 (Burfete's notes of June 2002 conversation with Bubb); Dep. of C. Bubb (AOL) at 61-62; Pls.' FOF ¶¶ 308-10.

179. On August 13, 2002, as a result of Informal Notice No. 5924, Verizon used DNS filtering to block access to a Web Server of a web host named Terra.es. Jt. Ex. 9, Tab A, line 407 (listing

Notice 5924); Dep. of S. Lebredo (Verizon) at 51-52, 55-58; Dep. of R. Heister (Verizon) at 18, 34-35, 45-46, 61; Pls.' Ex. 84 (August 16, 2002 letter from Verizon to OAG). Terra.es is "a large, commercial web hosting service," "web sites utilizing its services are all assigned the same IP address," and "upwards of 500,000 clients are assigned one IP number."[5] Pls.' Ex. 32 (Sep. 13, 2002 e-mail written by Burfete). All such web sites were blocked as a result of Verizon's compliance with Informal Notice 5924. Web sites for the following organizations hosted by Terra.es were among those blocked as a result of Informal Notice 5924: (1) the ITGE Geological Survey of Spain (http://www.terra.es/personal/lsomoza/marina/proyectos.html); and (2) the International Philatelic Club (http://www.terra.es/personal/jla31291/home.htm). Tr. 1/28/04 (Clark) pp. 25-27; Pls.' Ex. 104, Tab 9 (screenshots of the referenced web sites). The Attorney General acknowledged that these sites do not contain child pornography. Pls.' Ex. 74 (Def.'s Resp. to Pls.' First Set. of Interrogs.) ¶ 1.

180. On September 6, 2002, the OAG issued Informal Notice 1086 to AOL. As a result of that Informal Notice, AOL blocked access to IP address 217.116.4.196. Pls.' Ex. 46, p. 3 (internal AOL spreadsheet indicating that 217.116.4.196 was blocked in response to Informal Notice 1086); Jt. Ex. 9, Tab B, line 212 (listing Notice 1086). At least 546 web sites shared the IP address 217.116.4.196 as of January 24, 2004. Pls.' Ex. 96B (List of Web Sites that Resolved on 1/24/04 to IP Address Blocked in Response to Informal Notice 1086); Tr. 2/17/04 pp. 89-90

[5]Verizon used DNS filtering, not IP filtering, to disable access to the Terra.es online community. Thus, it would have been more accurate for Mr. Burfete to say that the 500,000 web sites were blocked by the DNS filter because they were sub-pages of the same domain name. However, because a domain name identifies a Web Server and all Web Servers have a unique IP address, all the sub-pages of a domain name share an IP address. FOF ¶¶ 22, 36. Thus, Mr. Burfete's statement is technically correct.

(description of Exhibit 96B); Tr. 1/27/04 pp. 180-82 (Clark).

181. AOL confirmed that, as of October 3, 2003, all of AOL's IP address blocks remained in place. Dep. of C. Bubb (AOL) at 140. As a result, the following constitutionally protected content is still being blocked as a result of Informal Notice 1086:

(1) http://isladeesculturas.tuportal.com/page2.html (a guide to the Spanish "Island of Sculptures" of Pontevedra); (2) http://cazurro.tuportal.com/webs/index.html (a directory of governmental, cultural, political, social, and tourist resources relating to the city of Leon, Spain); (3) http://club.imagenysonido.com/asetai/venticinco.htm (a Spanish translation of some writings of Chinese philosopher Tao Te Ching). Pls.' Ex. 5 (Third Report and Testimony of Michael Clark); Pls.' Ex. 96B (List of Web Sites that Resolved on 1/24/04 to IP Address Blocked in Response to Informal Notice 1086); Pls.' Ex. 104, Tab 11 (Screenshots of Referenced Web Sites); Tr. 1/7/04 pp. 183-99 (M.Clark). The Attorney General acknowledged that these sites do not contain child pornography. Pls.' Ex. 74 (Def.'s Resp. to Pls.' First Set of Req. for Admissions) ¶ 1. Mr. Clark also demonstrated in court that he was able to access two web sites that shared IP Address 217.116.4.196, isladeesculturas.tuportal.com and dragon.tuportal.com, through WorldCom, but he was not able to access those same sites through AOL, which had blocked them. Tr. 1/28/04 (Clark) pp. 163-69, 180, 182; Pls.' Exs. 109 (Screenshot of isladeesculturas.tuportal.com as accessed through WorldCom), 110 (Screenshot showing isladeesculturas.tuportal.com was not accessible through AOL), 111 (Screenshot showing dragon.tuportal.com not accessible through AOL), 116 (Screenshot of dragon.tuportal.com as accessed through WorldCom).

182. On November 4, 2002, the OAG issued Informal Notice 2966 to AOL. As a result of that

Informal Notice, AOL blocked access to IP address 207.44.156.52. Pls.' Ex. 97A (Informal Notice); Jt. Ex. 9, Tab B, line 154 (listing Notice 2966); Pls.' Ex. 46, p. 4 (internal AOL spreadsheet indicating that 207.44.156.52 was blocked in order to block access to the URL identified by Informal Notice 2966). At least 120 web sites shared the IP address 207.44.156.52 as of January 24, 2004. Pls.' Ex. 97B (List of Web Sites that Resolved on 1/24/04 to IP Address Blocked in Response to Informal Notice 2966); Tr. 1/27/04 pp. 185-87 (M.Clark). This IP address remained blocked by AOL as of the time of trial. Tr. 1/28/04 pp. 169-70, 176-77, 179-82. 183. On February 4, 2003, the OAG issued Informal Notice 1519 to Comcast. As a result of that Informal Notice, Comcast blocked access to IP addresses 202.181.231.211 and 202.181.231.212. Pls.' Ex. 98A (Informal Notice); Jt. Ex. 9, Tab B, lines 49-50 (listing Notice 1519). At least 3,988 web sites shared the IP addresses 202.181.231.211 and 202.181.231.212 as of November 2003. As of early January 2004, 3,962 sites still shared those IP addresses. Pls.' Ex. 80C (List of Web Sites that Resolved in November 2003 to IP Address Blocked in Response to Informal Notice 1086) ; Tr. 1/27/04 pp. 192-200 (M. Clark). Comcast confirmed that all of the IP addresses it blocked in response to Informal Notices remained in place as of October 23, 2003. Dep. of G. Lipscomb (Comcast) at 107.

184. On March 25, 2003, the OAG issued Informal Notices 1933 and 1947 to Comcast. As a result of those Informal Notices, Comcast blocked access to IP address 195.210.93.172. Pls.' Ex. 99A (Informal Notice No. 1933); Jt. Ex. 9, Tab B, lines 34-35 (listing Notices 1933 and 1947). A Web Hosting Service based in Italy, Digilander, uses IP address 195.210.93.172 for its digilander.libero.it domain. The Digilander site contains an index of the web sites that it hosts at this domain. According to this index, at least 342,080 web sites shared the IP address

195.210.93.172 as of November 2003. In early January 2004, the index listed 491,850 web sites at that IP Address. Pls.' Exs. 80D1, 80D2, 80D3 (List of 342,080 sub-sites Listed on the Digilander community site in late-November 2003); Tr. 1/27/04 pp. 203-05 (M. Clark); Tr. 1/28/04 pp. 3-6 (M. Clark).

185. On June 11, 2003, the OAG issued Informal Notice 2383 to Comcast. As a result of that Informal Notice, Comcast blocked access to IP address 213.59.0.84. Pls.' Ex. 100A (Informal Notice 2383); Jt. Ex. 9, Tab B, line 110 (listing Notice 2383). According to a list on the www.da.ru web site, www.da.ru hosted at least 331,066 web sites as of November 2003 and 334,395 web sites in early January 2004. In mid-February 2004, 326,650 web sites were listed as hosted at that IP address. Pls.' Exs. 80E1, 80E2 (List of 331,066 Web Sites of which on February 16th to 18th 2004 Approximately 271,000 Both Resolved to an IP Address Blocked by Comcast in Response to Informal Notice 2383 and also Redirected to Actual Content); Tr. 1/28/04 pp. 8-11 (M.Clark); Tr. 2/26/04 pp. 58-60 (M.Clark), pp. 69-70 (description of exhibit). One of the web sites blocked as a result of Informal Notices 2383 was http://dalmation.da.ru, an Ohio family's web site. Pls.' Ex. 80E1, p. 159; Pls.' Ex. 88 (Screen shot of dalmation.da.ru).

186. The OAG also sent Informal Notice 2384 targeting the same URL discussed in Finding of Fact 185 to Epix. Compare Jt. Exh. 9, Tab B, line 110 with Jt. Ex. 9, Tab B, line 111. As a result, Epix blocked access to the same web sites blocked by Comcast.

187. On June 11, 2003, the OAG issued Informal Notice 2386 to Comcast. As a result of that Informal Notice, Comcast blocked access to IP address 211.233.3.146. Pls.' Ex. 101A (Informal Notice 2386); Jt. Ex. 9, Tab B, line 113 (listing Notice 2386). Mr. Clark determined that 502 web sites shared the IP address 211.233.3.146 as of January 24, 2004. Pls.' Ex. 101B (List of 502

Web Sites That on 1/24/04 Resolved to an IP Address Blocked by Comcast on 6/18/03 in Response to Informal Notice 2386); Tr. 1/28/04 pp. 13-16 (M.Clark).

188. The OAG sent Informal Notice 2387 targeting the same URL discussed in Finding of Fact 187 to Epix. Compare Jt. Ex. 9, Tab B, line 113 with Jt.Exh. 9, Tab B, line 114. As a result, Epix blocked access to the same web sites blocked by Comcast.

189. Based on the evidence compiled by Mr. Clark, the total number of innocent web sites blocked by the Informal Notices discussed in this section is approximately 1,190,000. This number does not include the "upwards of 500,000" web sites hosted by Terra.es that were blocked by Verizon in compliance with Informal Notice 5924. FOF ¶ 179.

7. Notice and Review of Blocked Content

190. When WorldCom used IP filtering, it did not provide notice to the web site operators whose sites were affected. The web site operators had no way of knowing about the block unless they noticed that overall Internet traffic had decreased, researched the problem, and determined the reduction was attributable to the absence of queries from a particular ISP. Pls.' FOF ¶ 153; Dep. of C. Silliman (WorldCom) at 148-49.

191. The Act lacks any provision for subsequent or continuing review of the content located at the targeted URL to determine whether the URL continues to identify child pornography. Pls.' FOF ¶ 156.

192. In practice – consistent with the Act – the OAG did not undertake any later review to determine whether the content of a blocked URL had changed. Tr. 1/9/04 (Guzy Sr.) p. 97. The OAG conducted a review 30 days after the block was reported to verify that the URL was still blocked; such review did not cover the content of the blocked site. Pls.' FOF ¶ 157; Tr. 1/9/04

(Guzy Sr.) pp.128-29. The OAG conducted no other reviews or checks of blocked sites.

193. With the exception of several instances in which complaints were made about blocked innocent content, ISPs have continued to maintain the blocking action taken in response to the Informal Notices and the court order. For example, WorldCom continues to block IP addresses as a result of the court order it received. Tr. 1/27/04 (Krause) pp. 99-100. All of the IP address blocks instituted by Comcast in response to the Informal Notices remain in place. Dep. of G. Lipscomb (Comcast) at 107. AOL confirmed that its IP address blocks remain in place. Dep. of C. Bubb (AOL) at 140. Similarly, Verizon routinely maintains the blocks it placed in response to the Informal Notices. Dep. of S. Lebredo (Verizon) at 49; Pls.' FOF ¶ 393.

194. The ISPs maintain the blocks despite the fact that web site content can change frequently. For example, 45 of the web sites targeted by blocks implemented by AOL and Comcast no longer exist. Pls.' Ex. 6 (Fourth Report and Testimony of Michael Clark) ¶ 3; Tr. 1/8/04 (Clark) pp. 6-12; Pls.' FOF ¶ 394.

195. In addition to the 45 web sites that no longer exist, on December 1, 2003, 100 of the web sites tested by Mr. Clark resolved to a different IP address than the IP addresses that were blocked by AOL and Comcast in response to the Informal Notices. Pls.' Ex. 6 (Fourth Report and Testimony of Michael Clark) ¶ 3; Tr. 1/8/04 (Clark) pp. 6-12. Some of these 100 domain names no longer contain any child pornography. For example, Special Agent Dennis Guzy admitted that the content located at http://www.myfirstundressing.com is not child pornography and there is no law enforcement reason for that URL to remain blocked. Tr. 1/9/04 (Guzy Sr.) pp. 99-101; Pls.' Ex. 25A (Screenshot of content at this URL during trial). That URL was the subject of Informal Notice 3529 issued to AOL on May 28, 2002 and was blocked by AOL. Pls.' Ex. 25 (Informal

Notice 3529); Pls.' Ex. 74 (Def.'s Resp. to Pls.' First Set of Requests for Admission) ¶ 2. The web site is now located at a different IP address. Pls.' Ex. 74 ¶ 3 (Def.'s Resp. to Request for Admissions). Thus, it is now accessible through AOL's service. If AOL had used DNS filtering in response to that Informal Notice, the site would not be accessible through AOL's service even though it no longer contains child pornography. Tr. 1/28/04 (Clark) pp. 190-93; Pls.' FOF ¶¶ 398-400.

196. A wholly unrelated web publisher can acquire a domain name without any idea that the domain name is blocked by an ISP. For example, the URL http://www.littleangels.tv/tr was blocked by AOL in response to Informal Notice 4391. Pls.' Ex. 105A (Informal Notice 4391). In January of 2004, the domain name was made available for registration. CDT purchased and registered the domain name and created a web site located at the URL. Tr. 1/28/04 (Clark) pp. 46-61, 66. As demonstrated at trial, the web site now describes the actions taken by defendant pursuant to the Act and the instant litigation. Pls.' Ex. 104, Tab 14 (Screenshot of www.Little-Angels.tv web site). There is no means within the global domain name system for a future purchaser of an unused domain name to learn that the domain name is subject to a blocking order in Pennsylvania, and an innocent web publisher could pay to register a domain name with no idea – and no way to find out – that the domain was blocked by a major ISP. Tr. 2/18/04 (Stern) pp.17-19; Pls.' FOF ¶ 403.

8. Methods of Evasion

a. Anonymous Proxy Servers

197. Internet users who want to keep their identity secret can use anonymous proxy servers or anonymizers. In the context of visiting web sites, these services route all requests through the

proxy server or anonymizer, which in turn sends the request to the desired web site. Requests using these services appear to the ISP routing the request as if they are requests directed to the proxy service, not to the underlying URL to which the user actually seeks access. Pls.' FOF ¶ 132; Tr. 1/6/04 (Marcus) pp. 132-35.

198. The use of anonymous proxy services or anonymizers completely circumvents both of the technical blocking methods – IP filtering and DNS filtering – used by the ISPs to comply with the Informal Notices and would circumvent URL filtering as well. Tr. 1/6/04 (Marcus) pp. 134-35; Tr. 1/28/04 (Clark) pp. 76-79 (demonstrating use of proxy service); Tr. 2/18/04 (Stern) pp.13-14; Tr. 1/27/04 (Krause) pp. 33-34; Dep. of G. Lipscomb (Comcast) at 85-86; Dep. of R. Hiester (Verizon) at 36-37. For example, web sites blocked by AOL could be accessed through AOL's service using the anonymizer "Proxify.com." Tr. 1/7/04 (Clark) pp. 186-89; Pls.' Ex. 5 (Third Report and Testimony of Michael Clark) & Attachment C (demonstrating that site was blocked by AOL but that he was able to access it using Proxify.com); Pls.' FOF ¶¶ 493-495.

199. If the child pornography seeker chooses to have all of his web requests run through a proxy or anonymizer, he faces obstacles and risks. First, he must learn how to configure his computer to do so. This requires a number of difficult entries. Second, even if he successfully configures his computer, the seeker must then accept the risks of a reconfiguration that sends all requests through another computer that the user does not control – risks that the connection will not work or that the service will be slow. Tr. 1/29/04 (Stern) pp. 84-87; Tr. 1/7/04 (Marcus) pp. 39-40; Tr. 3/1/04 (Blaze) p. 76.

200. Individuals attempting to evade a DNS filter can do so by manually entering the IP address for a DNS server that is not controlled by their ISP. Tr. 1/7/04 (Smallacombe) p.119; Pls.' FOF

¶ 502.

b. The Ability of Child Pornographers to Evade Filters

201. Child pornographers can determine that blocking actions are being used – and that circumvention measures are needed – through customer complaints, by noticing a drop off in traffic from a particular ISP, or by establishing an account with an ISP suspected of blocking the web site and attempting to access the site through this service. Tr. 3/1/04 (Blaze) pp. 32-34.

202. IP filtering can be evaded by operators of child pornography sites by changing the IP address of the web site. Finding 140; Tr. 3/1/04 (Blaze) p. 26. In one instance, the OAG sent a second Informal Notice relating to one site because it had become available to AOL users at a different IP address after AOL blocked the original IP Address. AOL responded by blocking the second IP address as well. Dep. of C.Bubb (AOL) at 142-143; Pls.' Ex. 49 (Informal Notice 9851); Pls.' Ex. 46 page 2 (showing that AOL instituted a block of two different IP addresses on June 20, 2002 and August 5, 2002 for same URL).

203. Operators of child pornography sites can use a range of methods to evade DNS filtering, including: (1) using an IP address as a URL, i.e., a web site can use an IP address (or string of numbers) as the URL instead of a domain name like "www.example.com" (See supra FOF ¶ 161); or (2) changing a portion of a domain name and promulgating the new domain name in hyperlinks to the web site in advertisements, search engines or newsgroups. Tr. 3/1/04 (Blaze) pp. 28-29; Tr. 1/7/04 (Marcus) pp. 40-41.

9. Office of the Attorney General Response to Overblocking

204. The ISPs told the OAG at the April 2002 meetings that, with any method of blocking, they faced the problem of blocking non-child pornography content on the Internet. Specifically, they

reported that DNS filtering would block everything behind a given domain, and IP filtering would block everything associated with a given IP address. Dep. of C. Bubb at 44-46.

205. The OAG acknowledged that, before the first Informal Notice was sent to an ISP, the OAG knew that web sites shared IP addresses, Tr. 1/12/04 (Guzy Jr.) pp. 22-23, and that IP filtering risked blocking innocent web sites. Tr. 1/12/04 (Guzy Jr.) p.78. The OAG knew as early as May 17, 2002 that ISPs were using IP filtering to comply with Informal Notices. Pls.' Ex. 24 (May 17, 2002, compliance letter from Innernet.net stating that it had blocked four IP addresses in response to Informal Notices). Despite this knowledge, OAG did not take any steps to determine whether a web site shared its IP address with other sites before sending out an Informal Notice between March and September of 2003. Pls.' Ex. 73 (Def.'s Answers to Pls.' Third Req. for Prod. of Docs. and Interrogs.), ¶¶ 7-9, 14-15.

206. On a number of occasions, ISPs informed the OAG that compliance with the Informal Notices would block web sites that were not related to child pornography. In September 2002, after receiving the order to block Terra.es, WorldCom sent a letter to the OAG, explaining in great technical detail why this excessive blockage occurs. Tr. 1/9/04 (Burfete) p. 26; Jt. Ex. 8 (Sep. 23, 2002 letter from Craig Silliman to Burfete). In September 2002, AOL objected to the OAG's request to block Terra.es because it was concerned about the number of innocent sites that would be blocked, but the OAG continued to send Informal Notices directed at Terra.es. Pls.' Ex. 31 (Sep. 12, 2002 letter from AOL to OAG); Dep. of C. Bubb (AOL) at 73-82; Jt. Ex. 9 (Agreed Lists of Informal Notices), Tab B, Lines 430 (Informal Notice 5221 dated 10/4/02 directed at www.terra.es sub-domain), 433 (Informal Notice 3779 dated 10/4/02 directed at www.terra.es sub-domain).

207. Special Agent Dennis Guzy Sr. concluded on September 13, 2002, that OAG would never "be able to figure out all of the web hosting companies" (another term he used to describe Web Hosting Services). Pls.' Ex. 32 (Sep. 13, 2002 e-mail from Guzy Sr. to Burfete); Tr. 1/9/04 (Guzy Sr.) pp. 70-71. Although Agent Guzy reviewed every site before a Notice was sent and was able to recognize the names of "many" Web Hosting Services, he was not able to identify all Web Hosting Services. Pls.' Ex. 73 (Def.'s Answers to Pls.' Third Req. For Prod. of Docs. and Interrogs.) ¶ 12. For example, as discussed in Finding of Fact 209, Agent Guzy was not able to identify GeoCities as a Web Hosting Service before sending it an Informal Notice.

208. Starting in October 2002, the OAG began to use a different informal procedure with regard to content posted as a sub-page on a Web Hosting Service's web site. When Supervisor Guzy determined that a site displaying child pornography was a sub-page of one of these Web Hosting Services, he began sending a more abbreviated notice directly to the Web Hosting Service, generally asking it to take appropriate action. No records were kept of these notices in 2002. In 2003, Mr. Guzy sent approximately 70 of these notices. Jt. Stip. ¶ 57.

209. Despite this new procedure for implementing the Act when child pornography was found at sub-pages of Web Hosting Services, in February 2003 the OAG issued Informal Notices to Verizon, AOL and Erols asking that they block a subpage of the GeoCities.com online community, "a large hosting company." Jt. Ex. 9 (Agreed Lists of Informal Notices), Tab C, Lines 290, 319, 325 (Informal Notices 1643 (Erols), 1648 (AOL), 1647 (Verizon)).

F. IMPACT OF THE ACT ON INTERSTATE COMMERCE

210. Some ISPs were only able to implement blocking orders on a nationwide basis. Pls.' Ex. 9 (Mar. 20, 2002 e-mail from Guzy Sr. to Burfette). Some of these ISPs communicated this fact to

the OAG before the Act took effect. The OAG's Chief Information Officer, Peter Sand, recognized that implementation of the Act might extend outside of Pennsylvania, stating: "I think [the ISPs are] all distracted by their belief that they will have to make a technical distinction between [Pennsylvania] customers and their other customers. They might be technically unable to make that distinction. . . I think we may face a larger, legal problem by someone who might argue that what we are in fact doing is regulating 'stuff' outside of our geographic jurisdiction." Pls.' Ex. 8 (Mar. 19, 2002 e-mail from Sand to Burfete) at 2.

211. The blocking actions taken by AOL to comply with the Informal Notices were applied to AOL's entire global network and thus halted communications that took place entirely outside of Pennsylvania (and the U.S.). AOL told the OAG that it was "technologically incapable" of confining the impact of compliance with blocking orders to the Commonwealth of Pennsylvania. Pls.' Ex. 7 (March 18, 2002 e-mail from Burfete to Sand). Dep. of C. Bubb (AOL) at 125-26; Pls.' FOF ¶ 569.

212. The court order issued to WorldCom under the Act resulted in obstruction of communications on WorldCom's entire North American network. Dep. of C. Silliman (WorldCom) at 20, 97. This blocking affects all WorldCom customers in the United States and Canada and some WorldCom customers located overseas. As a hypothetical, a WorldCom customer in Minnesota would not be able to access a web site located in Georgia if it was blocked as a result of WorldCom's compliance with a Pennsylvania blocking order. Tr. 1/27/04 (Krause) pp.107-08. WorldCom informed the OAG that it was not technically feasible for it to block access only to Pennsylvania subscribers and that it would have to block access to all users of WorldCom's North American network. Jt. Ex. 8 (Sep. 23, 2002 letter from Silliman to Burfette)

p.3; Pls.' FOF ¶ 569.

213. Verizon informed the OAG about the interstate impact of blocking orders on its network. As Verizon explained, "blocking access to content or URLs accessible to Pennsylvania residents through Verizon-owned DNS servers requires Verizon also to block access to the same content and URLs by customers in other states who use these same DNS servers." Pls.' Ex. 84 (Aug. 16, 2002 letter from Verizon to OAG) at 2, note 2; Dep. of S. Lebredo (Verizon) at 42-44.

214. ISPs do not organize or design their internal networks along state boundaries, and thus it would be "extremely challenging" for an ISP to limit the impact of URL filtering to the State of Pennsylvania. Tr. 2/18/04 (Stern) pp. 85-86.

215. Even communications between Pennsylvanians are likely to be interstate communications. For example, all World Wide Web traffic of AOL's dial-up customers in Pennsylvania passes through an AOL data center located in Virginia. Dep. of B. Patterson (AOL) at 21; Pls.' FOF ¶ 573.

IV. CONCLUSIONS OF LAW

A. STANDING

1. CDT and ACLU

Plaintiffs CDT and ACLU have a right to receive information and interference with that right is an injury sufficient for standing. According to the Supreme Court, "[i]t is now well established that the Constitution protects the right to receive information and ideas," because the freedom of speech "necessarily protects the right to receive." Kleindienst v. Mandel, 408 U.S. 753, 762-763 (1972). On this issue, the Third Circuit has also ruled "[t]hat putative recipients of speech usually have standing to challenge orders silencing would-be speakers." Focus v.

Allegheny County Court of Common Pleas, 75 F.3d 834, 838 (3d Cir. 1996). However, the Third Circuit requires plaintiffs to demonstrate that the regulation of speech has "caused them injury in fact and that their injury is likely to be redressed by a favorable decision." Id. Defendant concedes that interference with the right to receive speech is a sufficient injury for standing. Def.'s Supp. Mem. at 11.

ACLU asserts standing on behalf of its members. "An association has standing to sue on behalf of its members when: (1) one of its members otherwise would have standing to sue on his own behalf; (2) the interests at stake are germane to the purpose of the organization; and (3) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit." Hill v. Park, No. 03-4677, 2004 U.S. Dist. LEXIS 1395, at *16 (E.D. Pa. Jan. 27, 2004) (citing Hunt v. Wash. State Apple Adver. Comm'n, 432 U.S. 333, 343 (1977)). "The Supreme Court has held that the third prong of this test is a prudential, not a constitutional, requirement." Id. (citing United Food & Commer. Workers Union Local 751 v. Brown Group, Inc., 517 U.S. 544, 557 (1996)).

CDT subscribes to WorldCom. FOF ¶ 96. WorldCom received a court order that directed it to block access to five URLs accessible through its service and used IP filtering to block access to two IP addresses in response. FOF ¶¶ 87, 92. There is no evidence of how many web sites were blocked by this action. However, given the Court's finding, based on the parties' stipulation, that at least fifty percent of domains share an IP address with at least fifty other domains, even if WorldCom's filtering did not result in overblocking, it is likely that WorldCom's response to future court orders would block content not targeted by the OAG. FOF ¶ 44. WorldCom was also ordered to block Terra.es, a large online community. WorldCom contacted

this company and had the offending material removed. FOF ¶ 92. If WorldCom had been unable to contact Terra.es in five days and had used IP filtering to block access to the IP address of Terra.es, hundreds of thousands of web sites not targeted by the court order would have been blocked. FOF ¶ 179.

ACLU members subscribe to, inter alia, AOL, Verizon, and Epix, all of which received Informal Notices and blocked access to the URLs specified by the notices, using either IP filtering, DNS filtering, or both. FOF ¶¶ 97, 157. As a result of the actions taken by these ISPs, ACLU members have been unable to access material available on the Internet. Specifically, Janet Goldwater testified that she was unable to access three web sites of interest to her that did not contain child pornography because they were blocked by her ISP, AOL. FOF ¶ 98. Most of the blocks implemented by the ISPs pursuant to the Informal Notices and, with respect to WorldCom an order, remained in place as of the time of the trial. FOF ¶ 193.

ACLU members and CDT have been injured by ISP compliance with the Informal Notices issued by the OAG and the court order obtained by the OAG because they have not been able to receive protected speech otherwise available on the Internet; they would be able to receive this speech if the blocks implemented by the ISPs are removed. Thus, they have standing to challenge the Act and the actions taken by the OAG to enforce the Act. ACLU also has standing on behalf of its members because (1) its members have standing; (2) the interests at stake are germane to the purpose of the organization – defending the principles of liberty and equality embodied in the Bill of Rights; and (3) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit.

2. PlantageNet

Defendant claims Plantagenet does not have standing because, although it is an ISP, it is an "insignificant operation that is hardly an ISP." Def.'s Opp'n at 10. According to defendant, although the OAG issued Informal Notices based on complaints from ISP customers, because Plantagenet has few customers, "no citizens will likely complain" to defendant about child pornography accessed through Plantagenet. Def.'s Supp. Mem. at 8.

A "credible threat" of enforcement is sufficient for standing. Planned Parenthood v. Farmer, 220 F.3d 127, 148 (3d Cir. 2000). Despite the fact that it outsources Internet access service, PlantageNet faces a credible threat of receiving an Informal Notice or court order under the Act. PlantageNet has customers in Pennsylvania who could file a citizen complaint with the OAG if they discovered child pornography on the Internet. FOF ¶ 58. Because Plantagenet's customers have not been informed of the fact that PlantageNet outsources its Internet access services, any complaint they made to the AOG about child pornography would identify PlantageNet as their ISP. FOF ¶ 99. The supervisor and legal adviser for the CSEU both testified that they consider PlantageNet an ISP and that, upon receipt of a complaint and verification, they would issue an Informal Notice to PlantageNet and expect it to comply. FOF ¶ 100. Thus, PlantageNet faces a credible threat of enforcement and has standing to challenge the Act and the OAG's enforcement action.

3. Overbreadth

Plaintiffs argue that the Act is unconstitutionally overbroad because it suppresses a substantial amount of protected speech. Pls.' Mot. at 31. In addition to this substantive argument, plaintiffs contend that the overbreadth doctrine provides them with standing to

represent absent parties affected by the Act who are unable or unwilling to challenge the Act. Pls.' Mot. at 23.

In order to succeed on an overbreadth challenge, plaintiffs must show that the law, on its face, "punishes a 'substantial' amount of protected free speech, 'judged in relation to the statute's plainly legitimate sweep.'" Virginia v. Hicks, 539 U.S. 113, 118-119 (2003) (quoting Broadrick v. Oklahoma, 413 U.S. 601, 615 (1973)). The overbreadth doctrine, however, should be used "sparingly and only as a last resort." Broadrick, 413 U.S. at 613.

The Supreme Court has altered its traditional rules of standing by not requiring a plaintiff asserting an overbreadth challenge to "demonstrate that his own conduct could not be regulated by a statute drawn with the requisite narrow specificity." Id. at 612 (quoting Dombrowski v. Pfister, 380 U.S. 479, 486 (1965)). This exception to traditional rules of standing is justified by a concern that an overbroad law will "chill" protected speech or that "persons whose expression is constitutionally protected may well refrain from exercising their right for fear of criminal sanctions provided by a statute susceptible of application to protected expression." ACLU v. Ashcroft, 322 F.3d 240, 266 (3d Cir. 2003).

Application of the overbreadth doctrine is not justified in this case. First, overbreadth is a facial challenge to a statute. Plaintiffs do not argue that the Act, on its face, punishes protected speech or that any of the URLs targeted by the Informal Notices identified a web page that did not contain child pornography. The Pennsylvania definition of child pornography, set forth in Appendix B, is similar to the definition found constitutional by the Supreme Court in New York

v. Ferber, 458 U.S. 747 (1982) and has been applied in this district.[6] See United States v. Cochran, 806 F. Supp. 560, 564 (E.D. Pa. 1992).[7] Second, plaintiffs do not assert that, on its face, the Act chills any protected speech. In fact, plaintiffs claim that most web-site operators are not even aware of the fact that their web-sites are blocked. FOF ¶¶ 171-75 (detailing process Laura Blain needed to go through to find out why site was blocked), 190.

Although implementation of the Act has resulted in the suppression of protected speech, the Court cannot conclude that the Act is invalid on its face or that the Act has, on its face, chilled any protected expression. As a result, plaintiffs' overbreadth challenge cannot succeed and they are not entitled to overbreadth standing.

B. SUBSTANTIVE FIRST AMENDMENT ISSUES

The Supreme Court has stated, "[t]hrough the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer." Reno v. ACLU, 521 U.S. 844, 870 (1997). As a result, the Court has ruled that there is "no basis for qualifying the level of First Amendment scrutiny that should be applied to

---

[6]The statute at issue in Ferber criminalized, inter alia, taking a picture of a child less than sixteen years of age engaged in a sexual conduct. Sexual conduct was defined as "actual or simulated sexual intercourse, sexual bestiality, masturbation, sado-masochistic abuse, or lewd exhibition of the genitals." Ferber, 458 U.S. at 750. The Pennsylvania child pornography definition applies to children under the age of eighteen and defines sexual conduct as "sexual intercourse . . ., 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.A. § 6312.

[7]Although plaintiffs argue that the "for the purpose of sexual stimulation" language in the statutory definition of child pornography is vague, the Court agrees with the statement of the Cochran court that this language can, and must, be interpreted to be consistent with Ferber. Cochran, 806 F. Supp. at 563 n. 2.

this medium." Id.

1. Burden on Speech

Defendant proposes that the "only reasonable means" test should be used to determine whether the Act burdens speech. Under defendant's test, the Act is constitutional unless the only reasonable means of compliance requires blocking protected speech. Plaintiffs argue that if the effect of the Act has been to block protected speech, the Act is subject to First Amendment scrutiny.

This case is unusual in that the Act, on its face, does not burden protected speech. See supra Section IV(A)(3). Facially, the Act only suppresses child pornography, which can be completely banned from the Internet.[8] See ACLU v. Reno, 929 F. Supp. 824, 865 (E.D. Pa. 1996) ("The Government could also completely ban obscenity and child pornography from the Internet."). However, the action taken by private actors to comply with the Act has blocked a significant amount of speech protected by the First Amendment. United States v. Playboy Entertainment Group, 529 U.S. 803 (2000), relied upon by both parties, is the case that comes closest to addressing how this type of burden on protected speech should be addressed.

The federal statute at issue in Playboy required cable operators which provided sexually oriented programing to either fully scramble or block the channels that provided this

---

[8]In Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002), the Supreme Court held that "virtual" (or computer generated) child pornography was subject to closer scrutiny than pornography made with actual children. Id. at 241; see supra § IV.B.2 for a more complete discussion of this case. The statute in Ashcroft prohibited a visual depiction that "is, or appears to be, of a minor engaging in sexually explicit conduct." In contrast, Pennsylvania's definition of child pornography is limited to "material depicting a child under the age of 18 years engaged in a prohibited sexual act." ; 18 Pa. Cons. Stat. § 6312. The Court concludes the Pennsylvania definition does not cover "virtual" child pornography.

programming, or limit the transmission of such programming to the hours between 10:00 P.M., and 6:00 A.M., referred to as "time channeling." Id. at 806. The Supreme Court determined that the statute was unconstitutional because the government failed to establish that the two methods for compliance identified in the challenged section were the least restrictive means for achieving the government's goal. In addressing the statute, the Playboy Court applied strict scrutiny because the speech targeted was defined by its content - "sexually explicit content." Id. at 811.

The analysis of the Playboy Court is particularly instructive in this case. That is so because the majority of cable operators involved in that case chose to comply with the section of the statute at issue by using time channeling notwithstanding the fact that it silenced a significant amount of protected speech, whereas the other stated method of compliance, scrambling, did not. Id. at 806. On that issue, the Court ruled that a reasonable cable operator could choose not to use the scrambling alternative provided by the statute because the available scrambling technology was "imprecise" and portions of the scrambled programs could be heard or seen by viewers, a phenomenon known as "signal bleed." Thus, "[a] rational cable operator, faced with the possibility of sanctions for intermittent bleeding, could well choose to time channel even if the bleeding is too momentary to pose any concern to most households." Id. at 821. The Court also noted that digital technology would have solved the signal bleed problem, but it was "not in wide-spread use."

The basis for the Playboy Court's determination that the statute was not the least restrictive means for achieving the government's goal was the fact that time channeling, deemed to be a reasonable method of compliance for cable operators, silenced "protected speech for two-thirds of the day in every home in a cable service area, regardless of the presence or likely

presence of children or of the wishes of viewers." Id. In making this statement, the Court determined that "targeted blocking" at the request of a customer was a "less restrictive" and feasible means of furthering the government's compelling interest in the case.[9] Id. at 816, 827. Targeted blocking required cable operators to block sexually - oriented channels at individual households. It was deemed to be less restrictive in that it enabled parents who did not want their child exposed to the program to block the offending channels without depriving willing viewers of the opportunity to watch a particular program. Id. at 815.

The Act in this case has resulted in the blocking of in excess of 1,190,000 web sites that were not targeted by the Informal Notices. FOF ¶¶ 170, 178-89. Defendant argues that this overblocking does not violate the First Amendment because it resulted from decisions made by ISPs, not state actors. According to defendant, ISPs have "options for disabling access that would and will not block any, or as many, sites as Plaintiffs claim were blocked in the past" and the choice of which filtering method to use was "completely the decision of the ISPs." Def.'s Opp'n at 51.

The Court rejects this argument. Like the statute analyzed in Playboy, the Act in this case provides ISPs with discretion to choose a method of compliance although such methods are not incorporated in the Act itself. Like the time channeling in Playboy, the court concludes that ISPs could reasonably choose IP filtering and DNS filtering in order to comply with Act. And, like Playboy, the alternatives reasonably available to the ISPs block protected speech to a significant degree.

---

[9]The Court notes that targeted blocking was a means of compliance identified in another section of the statute that was not challenged. Playboy, 529 U.S. at 809-10.

The two filtering methods used by the ISPs to comply with the Informal Notices and the court order – IP filtering and DNS filtering – both resulted in overblocking. IP filtering blocks all web sites at an IP address and, given the prevalence of shared IP addresses, the implementation of this method results in blocking of a significant number of sites not related to the alleged child pornography. FOF ¶¶ 140-41. As an example, access to Ms. Blain's web sites and over 15,000 other sites was blocked to Epix users as a result of the IP Filtering Epix implemented to comply with Informal Notice 2545. FOF ¶ 170. DNS filtering also results in overblocking when the method is used to block a web site on an online community or a Web Hosting Service, or a web host that hosts web sites as sub-pages under a single domain name. FOF ¶¶ 137-39. Specifically, Verizon blocked hundreds of thousands of web sites unrelated to the targeted child pornography when it used DNS filtering to block access to a sub-page of the Terra.es web site, a large online community, in response to Informal Notice 5924. One of the web sites blocked was for a Spanish geological survey, and defendant acknowledged that this web site did not contain child pornography. FOF ¶ 179. Although a small subset of web hosts, Web Hosting Services host a large number of web sites and the OAG admitted that they are not always identifiable based on the URL. In fact, the OAG continued to issue notices to Web Hosting Services after it was aware of the overblocking problem and had implemented a new procedure to deal with these services. FOF ¶¶ 207-209.

Moreover, contacting the web host is not a legitimate alternative to use of technical filtering methods. ISPs will not always be able to contact the host within the time period provided by the Act. Even if they can contact a host, the host may not be willing to remove the offending content. In either event, the ISP would be forced to use IP filtering or DNS filtering to disable

access. In addition, an ISP using this method of compliance risks criminal prosecution if the host decides to place the offending content back on the Internet. Thus, it is rational for an ISP to implement a method of compliance that is not based on the actions of a third party.

The Court will evaluate the constitutionality of the Act with respect to the technology that is currently available. The Playboy Court did not consider digital technology a feasible alternative because it was not "economical" for cable operators to use this technology. Similarly, in Reno v. ACLU, 521 U.S. 844 (1997), the Supreme Court rejected an argument that Internet content providers could rely on "tagging" or credit card verification technology because the proposed screening software did not exist at that time. Id. at 881-82. According to the Court, the "District Court correctly refused to rely on unproven future technology to save the statute." Id. at 882; see also Reno v. ACLU, 521 U.S. 844, 891 (1997) (O'Connor, J., concurring) ("Although the prospects for the eventual zoning of the Internet appear promising, I agree with the Court that we must evaluate the constitutionality of the CDA as it applies to the Internet as it exists today.")

The URL filtering technology recommended by the OAG at trial was not available to any ISPs that received Informal Notices or a court order, with the exception of AOL. AOL's use of URL filtering was limited; it could not use URL filtering on its entire network. FOF ¶¶ 123-25. The evidence establishes that it would not be economical for ISPs to develop and implement URL filtering technology. Even if the ISPs invested in the development of this technology, it would take a significant amount of research and testing to implement this filtering method and none of the experts or engineers who testified were able to give a timetable for the completion of this research. FOF ¶¶ 125-26. Moreover, if the ISPs were able to develop the devices and software necessary to perform URL filtering, they would be required to purchase "substantially more"

switches and routers to avoid "significantly" degrading the performance of their networks. FOF ¶¶ 124-26. Given the uncertain nature of the research, it is difficult to predict the cost of developing this technology. However, one expert estimated that it would cost the ISP that employs him, Verizon, "well into seven figures" to implement URL filtering across its entire network. FOF ¶ 126. Thus, URL filtering is not a feasible alternative to DNS filtering and IP filtering.

As this Court reads Playboy, if a statute regulating speech provides distributors of speech with alternatives for compliance and the majority of distributors reasonably choose an alternative that has the effect of burdening protected speech, the statute is subject to scrutiny as a burden on speech. Both of the filtering methods used by the ISPs in response to Informal Notices and the court order issued in this case resulted in the blocking of innocent speech. The method of filtering recommended by defendant at trial – URL filtering – was rejected by the ISPs as infeasible. As a result, the Court concludes that the Act burdens speech and is subject to First Amendment scrutiny.

2. Level of Scrutiny

In determining whether a statute's burden on protected speech is constitutional, a Court must generally first decide whether to apply strict or intermediate scrutiny. Plaintiffs argue that strict scrutiny applies because the Act is a content based restriction on speech. Pls.' Supp. Mem. at 29. Defendant argues that intermediate scrutiny is more appropriate because the Act only applies to child pornography, which has no protection, and the burden on protected expression is a collateral consequence of the Act. In addition, defendant argues that intermediate scrutiny applies because the Act regulates conduct – child sexual abuse – or the secondary effects of the

manufacture of child pornography – also child sexual abuse. Def.'s Supp. Mem. at 42.

The Supreme Court generally subjects "regulations that suppress, disadvantage, or impose differential burdens upon speech because of its content" to strict scrutiny. "In contrast, regulations that are unrelated to the content of speech are subject to an intermediate level of scrutiny because in most cases they pose a less substantial risk of excising certain ideas or viewpoints from the public dialogue." Turner Broad. Sys. v. FCC, 512 U.S. 622, 642 (1994). "Strict scrutiny requires that a statute (1) serve a compelling governmental interest; (2) be narrowly tailored to achieve that interest; and (3) be the least restrictive means of advancing that interest." ACLU v. Ashcroft, 322 F.3d 240, 251 (3d Cir. 2003) (quoting Sable, 492 U.S. at 126)). Intermediate scrutiny is more difficult to define. According to the Third Circuit, "[a]dmittedly, the intermediate scrutiny test applied varies to some extent from context to context, and case to case. But it always encompasses some balancing of the state interest and the means used to effectuate that interest. Bartnicki v. Vopper, 200 F.3d 109, 124 (3d Cir. 1999). As set forth by the Supreme Court in United States v. O'Brien, 391 U.S. 367 (1968), intermediate scrutiny requires that a regulation "(1) furthers an important or substantial governmental interest; (2) the governmental interest is unrelated to the suppression of free expression; and (3) the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest." Id. at 377.

The Supreme Court has acknowledged that "[d]eciding whether a particular regulation is content-based or content-neutral is not always a simple task." Turner Broad. Sys., 512 U.S. at 642. In Turner Broadcasting Systems, the Court stated that "principal inquiry in determining content-neutrality . . . is whether the government has adopted a regulation of speech because of

[agreement or] disagreement with the message it conveys." Id.

Even if a statute is content-based, it is not always subject to strict scrutiny because this general rule is subject to "narrow and well-understood exceptions." ACLU v. Reno, 929 F. Supp. 824, 865 (E.D. Pa.. 1996) (quoting Turner Broadcating, 512 U.S. at 641). There are exceptions for obscenity, as defined in Miller v. California, 413 U.S. 15 (1973), and child pornography, detailed in New York v. Ferber, 458 U.S. 747 (1982). Id. Based on these exceptions, defendant could "completely ban obscenity and child pornography from the Internet. No Internet speaker has a right to engage in these forms of speech, and no Internet listener has a right to receive them." Id. (citing Alliance for Community Media v. FCC, 56 F.3d 105, 112 (D.C. Cir. 1995)).

The exception for child pornography can be explained, in part, by the fact that the regulation of child pornography is not based on a disagreement with the message conveyed by this material; thus, the typical justification for strict scrutiny is not applicable. In New York v. Ferber, 458 U.S. 747, 763-764 (1982), the Court held that child pornography was unprotected speech subject to content-based regulations. Id. at 765 n.18. The Court in Ferber concluded that the statute was not justified by any disagreement with the message conveyed by the content but by "the prevention of sexual exploitation and abuse of children." Id. at 757. As a result, child pornography was classified "as a category of material outside the protection of the First Amendment." Ferber, 458 U.S. at 763.

In Ashcroft v. Free Speech Coalition, 535 U.S. 234, 250 (2002), the Court declared that a statute banning "virtual" (or computer generated) child pornography was unconstitutional. In doing so the Court reiterated that suppression of child pornography is not justified by a disagreement with the message conveyed by the material. It is only "where the images are

themselves the product of child sexual abuse [that] Ferber recognized that the state had an interest in stamping it out without regard to any judgment about its content. The production of the work, not its content, was the target of the statute." Id. at 249. The Ashcroft ruling was based on the fact that, although the distribution and sale of child pornography are "intrinsically related" to the sexual abuse of children, that is not the case with the production of "virtual" child pornography which does not involve actual children.

The fact that virtual child pornography is not intrinsically related to child abuse also explains why the Ninth and First Circuits decided to apply strict scrutiny to a child pornography law that banned virtual child pornography in Free Speech Coalition v. Reno, 198 F.3d 1083 (9th Cir. 1999) and United State v. Hilton, 167 F.3d 61 (1st Cir. 1999) – the cases relied upon by plaintiffs. As explained by the Ninth Circuit, the regulation in Free Speech Coalition "shifted from defining child pornography in terms of the harm inflicted upon real children to a determination that child pornography was evil in and of itself, whether it involved real children or not." Id. at 1089.

In contrast, the Act at issue in this case, on its face, only regulates material that is "outside the protection of the First Amendment." If it were not for the fact that the implementation of the Act resulted in the suppression of protected speech, the Act would not be subject to First Amendment scrutiny. Furthermore, there is no evidence that the innocent content blocked by implementation of the Act is suppressed because of its content or a disagreement with the message it conveys. To the contrary, there is no evidence that the OAG knew the content of the innocent web sites blocked by the ISPs or had any reasonable method of obtaining such information. FOF ¶ 47. As a result, the traditional justifications for strict scrutiny do not apply.

Defendant has a strong argument that intermediate scrutiny should apply. The Act is aimed at a legitimate subject of regulation – child pornography – but has the incidental or collateral effect of burdening speech. Although there are no cases directly on point, this statute's collateral or incidental effect on protected speech is similar to the burden on speech in cases in which intermediate scrutiny was applied. For example, the burden on speech is similar to the one upheld in a secondary effects case, Renton v. Playtime Theatres, Inc., 475 U.S. 41, 48 (1986), in which the Court allowed "differential treatment to . . . a content-defined subclass of proscribable speech" because "the subclass [was] associated with particular 'secondary effects' of the speech, so that the regulation [was] 'justified without reference to the content of the speech." In Renton, a statute providing for the zoning of adult movie theaters was justified as an attempt to reduce the "adverse effects" such theaters had on the surrounding area. These adverse effects included harm to neighborhood children and community improvement efforts. Id. at 51. Similary, the Act is aimed at the "adverse effects" of the production of child pornography – the exploitation and abuse of children. Moreover, the Act is not aimed at suppressing the message communicated by child pornography, it is justified by Pennsylvania's interest in protecting children from sexual exploitation. Thus, the regulation is based on how the material "[is] made, not on what it communicate[s]." Ashcroft, 535 U.S. at 251.

One other court applied intermediate scrutiny to a child pornography regulation. In American Library Ass'n v. Thornburgh, 713 F. Supp. 469 (D.D.C. 1989), the Court applied intermediate scrutiny to a law imposing record-keeping requirements on film-makers to prevent child pornography. According to the court, "The key in determining the constitutionality of a law that 'spills over' from a legitimate governmental interest – such as the effort against child

pornography – onto protected material is whether the legislation is 'narrowly drawn' to avoid as much interference with protected material as possible while furthering the legitimate governmental interest. Courts must be especially vigilant in scrutinizing broad legislative efforts that clearly burden protected First Amendment material in the name of attacking things not constitutionally protected." Id. at 477.

Although there are strong arguments for the application of strict and intermediate scrutiny, the Court need not choose between the two because, even under the less demanding standard – intermediate scrutiny – the Act does not pass Constitutional muster. Under O'Brien, a regulation must further an important government interest unrelated to the suppression of free expression and the incidental restriction on First Amendment freedoms must be no greater than is essential to the furtherance of that interest. O'Brien, 391 U.S. at 377. The government has the burden of proving that the "regulation will in fact alleviate [the] harms [addressed by the regulation] in a direct and material way," Turner, 512 U.S. at 664, and it has not met that burden in this case. In addition, the Act suppresses substantially more protected material than is essential to the furtherance of the government's interest in reducing child sexual abuse.

Although the prevention of child exploitation and abuse is an state interest unrelated to the suppression of free expression, defendant has not produced any evidence that the implementation of the Act has reduced child exploitation or abuse. The Act does block some users' access to child pornography; however, the material is still available to Internet users accessing the material through ISPs other than the one that blocked the web site. FOF ¶ 109. In addition, there are a number of methods that users and producers of child pornography can implement to avoid the filtering methods. FOF ¶¶ 197-20. For example, both IP filtering and DNS filtering can be

avoided by a person using an anonymous proxy server or an anonymizer. FOF ¶¶ 197-99. A child pornographer can evade an IP filter by moving his web site to another IP address without having to change the content or the URL identifying the site. FOF ¶ 202. A user attempting to evade a DNS filter can manually enter the IP address for a DNS server not controlled by his ISP to avoid the block. FOF ¶ 200. Moreover, there is no evidence that any child pornographers have been prosecuted as a result of defendant's enforcement of the Act. In fact, the OAG did not investigate the entities that produce, publish, and distribute the child pornography. FOF ¶ 69. Although the inference could be drawn that making it more difficult to access child pornography reduces the incentive to produce and distribute child pornography, this burden on the child pornography business is not sufficient to overcome the significant suppression of expression that resulted from the implementation of the Act.

More than 1,190,000 innocent web sites were blocked in an effort to block less than 400 child pornography web sites, and there is no evidence that the government made an effort to avoid this impact on protected expression. FOF ¶ 189. As discussed in the previous section of this Memorandum, all the currently available technical methods of disabling access to a web site accessible through an ISP's service result in significant overblocking. The Act fails to specify any means of compliance, let alone provide guidance as to which method will minimize or avoid suppression of protected speech. This burden on protected expression is substantial whereas there is no evidence that the Act has impacted child sexual abuse. Thus, the Act cannot survive intermediate scrutiny.

The Act requires ISPs to block child pornography "residing on," as well as "accessible through," their service. The overblocking only occurs with respect to filtering utilized to block

child pornography accessible through an ISP's service. The overblocking problem is not encountered when an ISP removes content residing on its service because an ISP can remove such content without affecting any other content. FOF ¶¶ 144-45. Thus, defendant argues that the "accessible through" provision can be severed from the Act, leaving the "residing on" provision of the Act in place. It is unnecessary for the Court to address the severability argument because it concludes in the next section of this Memorandum that the procedural safeguards provided in the Act are insufficient under the Constitution.

C. PROCEDURAL FIRST AMENDMENT ISSUES

1. Prior Restraint

The Act and Informal Notice process are not prior restraints in the traditional sense. They do not prevent speech from reaching the market place but remove material already available on the Internet from circulation. Alexander v. United States, 509 U.S. 544 (1993) ("The term 'prior restraint' describes orders forbidding certain communications that are issued before the communications occur.") However, they are administrative prior restraints as that term has been interpreted by the Supreme Court. According to the Court, "only a judicial determination in an adversary proceeding ensures the necessary sensitivity to freedom of expression, only a procedure requiring a judicial determination suffices to impose a valid final restraint." Freedman v. Maryland, 380 U.S. 51, 58 (U.S. 1965). Thus, if material protected by the First Amendment is removed from circulation without these procedural protections, the seizure is invalid as a prior restraint. The Court used the term to describe a Rhode Island Commission's practice of sending letters to book distributors that asked the distributors to remove books from circulation in Bantam Books v. Sullivan, 372 U.S. 58 (1962) and a procedure that allowed courts to order pre-trial

seizure of films alleged to be obscene in Fort Wayne Books, Inc. v. Indiana, 489 U.S. 46, 51-52 (1989).

In Bantam Books, the Court ruled on a regulatory scheme implemented by the state of Rhode Island. The state created the Rhode Island Commission to Encourage Morality in Youth, and this commission sent book distributors letters informing them that books they were distributing were "objectionable" and asking them to "cooperate" by removing this material from book stores. Id. at 61-63. The letters also stated that "the Attorney General will act for us in the case of non-compliance." Id. at 63. In response, plaintiffs stopped further circulation of copies and "instructed field men to visit retailers and to pick up all unsold copies." Although these materials were already in circulation, the Court referred to this system as a "prior administrative restraint" and ruled it was unconstitutional because there was not "an almost immediate judicial determination of the validity of the restraint" and the publisher or distributor was not entitled to notice and a hearing.

In Fort Wayne Books v. Indiana, 489 U.S. 46 (1989), the Court held that a finding of probable cause by a state court was not sufficient to allow seizure of material "presumptively protected by the First Amendment." "While a single copy of a book or film may be seized and retained for evidentiary purposes based on a finding of probable cause, the publication may not be taken out of circulation completely until there has been a determination of obscenity after an adversary hearing." Id. at 63. Like Bantam Books, the materials in Fort Wayne were already in circulation. They were removed from circulation by a state court order. According to the Court, "our cases firmly hold that mere probable cause to believe a legal violation has transpired is not adequate to remove books or films from circulation." Ft. Wayne Books v. Indiana, 489 U.S. 46,

66 (1989).

Based on the decision in Bantam Books and Fort Wayne Books, this Court concludes the procedural protections provided by the Act are inadequate. These cases require a court to make a final determination that material is child pornography after an adversary hearing before the material is completely removed from circulation. Under the Act, a judge is only required to make a finding of probable cause, he can make this determination ex parte, and there is no requirement that the publisher or distributor receive notice or an opportunity to be heard. FOF ¶¶ 51-54, 80-82.

Additionally, as argued by plaintiffs, the Act allows for an unconstitutional prior restraint because it prevents future content from being displayed at a URL based on the fact that the URL contained illegal content in the past. Pls.' Mot. at 25-26. Plaintiffs compare this burden to the permanent ban on the publication of a newspaper with a certain title, Near v. Minnesota, 283 U.S. 697 (1931), or a permanent injunction against showing films at a movie theater, Vance v. Universal Amusement Co., 445 U.S. 308 (1980). In Near, the Court examined a statute that provided for a permanent injunction against a "malicious, scandalous, and defamatory newspaper, magazine or other periodical." Near, 283 U.S. at 701-702. Near involved a county attorney who obtained an injunction against the publishers of a newspaper called "The Saturday Press" under a statute preventing them from "publishing, circulating, or having in their possession any future editions of said The Saturday Press." Id. at 705. The statute at issue in Near was held to be unconstitutional because it permitted censorship of future publications based on material published in the past. See Universal Amusement Co. v. Vance, 404 F. Supp. 33, 44 (S.D. Tex. 1975) ("In both [Near and Vance] the state made the mistake of prohibiting future conduct after a

finding of undesirable present conduct.").

There are some similarities between a newspaper and a web site. Just as the content of a newspaper changes without changing the title of the publication, the content identified by a URL can change without the URL itself changing. FOF ¶ 24. In fact, it is possible that the owner or publisher of material on a web site identified by a URL can change without the URL changing. Plaintiffs demonstrated this by purchasing the http://www.littleangels.tv/tr URL and converting the alleged child pornography web site into a web site dedicated to a description of this case. FOF ¶ 196. Moreover, an individual can purchase the rights to a URL and have no way to learn that the URL has been blocked by an ISP in response to an Informal Notice or court order. FOF ¶ 196. Despite the fact that the content at a URL can change frequently, the Act does not provide for any review of the material at a URL and, other than a verification that the site was still blocked thirty days after the initial Informal Notice, the OAG did not review the content at any blocked URLs. FOF ¶ 191-92. Moreover, other than the instances in which complaints were made about blocked innocent content, ISPs have continued to maintain their blocking action. Specifically, WorldCom, Comcast, AOL, and Verizon all testified that they routinely maintain the blocks implemented in response to Informal Notices or, with respect to World Com, the court order. FOF ¶ 193.

Defendant argues that it is not necessary to hold an adversary hearing before material is removed from circulation because the criminal trial that must be held before an ISP can be convicted will provide the procedural due process required by the First Amendment. Def.'s Supp. Mem. at 10. The Court rejects this argument. A similar argument was rejected by the Supreme Court in Freedman v. Maryland, 380 U.S. 51 (1965), an obscenity case. In that case, the Court

held that a statute that required a theater owner to receive a license before exhibiting a film was unconstitutional because the statute did not, inter alia, "assure a prompt final judicial decision" that the film was obscene. Id. at 59-60. The Act does not provide for any review of a judge's ex parte determination that a web site contains child pornography.

Defendant misses the mark when he focuses on the fact that criminal liability will not be imposed until after a criminal trial. The Court's First Amendment analysis must focus on when speech is suppressed and, under the Act, speech is suppressed when the court order is issued. Under the First Amendment, more procedures are necessary before speech can be suppressed than are required before an individual can be arrested. Although evidence of probable cause is sufficient to make an arrest, Fort Wayne holds that a finding of probable cause is not sufficient to completely remove a publication from circulation. As explained by the Seventh Circuit, "[w]hile at first glance it may seem odd to require more judicial protection for the liberty of one's books than for one's body, the distinction reflects this country's great concern with the chilling effect on protected speech brought on by a government seizure." United States v. Moore, 215 F.3d 681, 685 (7th Cir. 2000).

The fact that an ISP can challenge a judge's child pornography determination in a criminal prosecution does not save the Act. Only one ISP, WorldCom, challenged an Informal Notice and then promptly complied with a court order obtained by the OAG. An ISP has little incentive to challenge the suppression of a web site with which it has no business relationship. As stated by the Supreme Court, a statute that suppresses speech "must be tested by its operation and effect." Near v. Minnesota, 283 U.S. 697, 708 (1931). The operation and effect of this Act is that speech will be suppressed when a court order is issued, and the procedural protections provided by the

Act before the order can issue are insufficient to avoid constitutional infirmity.

2. Child Pornography vs. Obscenity

Defendant argues that fewer procedural protections are required for the removal from circulation of child pornography, as compared with obscenity, because the child pornography determination is easier than the obscenity determination. The Court rejects this argument.

This argument is based on defendant's position that Fort Wayne Books was distinguished in dicta by Camfield v. City of Oklahoma City, 248 F.3d 1214, 1227 (10th Cir. 2001). According to the court in Camfield, "we do not necessarily agree with the implication that compliance with Fort Wayne Books is always required whenever the government seeks to remove suspected child pornography from public access." Id. "Child pornography differs from obscenity in two important respects. First, child pornography is afforded even less constitutional protection than obscenity. Second, as courts have noted in the context of probable cause determinations, the difficulty encountered in determining whether material is obscene often is absent when determining whether material contains child pornography." Id. For example, with child pornography a court does not have to assess whether the work, "taken on the whole, contains serious literary, artistic, political, or scientific value." See New York v. Ferber, 458 U.S. 747, 761, 764 (1982). However, the Camfield court did not reach the issue because the child pornography statute examined in that case did require an examination of the artistic merit of the work as a whole, and the court held that the difficulty in making this assessment rendered compliance with Fort Wayne Books necessary. Id. at 1228. The court noted, however, that the appellant "does not cite, nor have we found, any cases which have held that the complete removal of suspected child pornography from public circulation without a prior adversarial hearing

constitutes a prior restraint." Id.

Camfield was decided before the Supreme Court's decision in Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002). Ashcroft affects this Court's analysis of Camfield in two respects. First, the Supreme Court acknowledged in Ashcroft that virtual pornography is indistinguishable from real child pornography. Ashcroft v. Free Speech Coalition, 535 U.S. 234, 254 (2002) ("Experts, we are told, may have difficulty in saying whether the pictures were made by using real children or by using computer imaging."). Second, the Court held that virtual child pornography can be protected speech. Both of these statements make a child pornography determination more difficult because a court now must assess whether the alleged child pornography is virtual. Pls.' Reply at 30-31. In a case decided after Ashcroft, the First Circuit affirmed a decision to vacate a conviction for possession of child pornography because the government did not present evidence proving that the child in the image was "not confabulated, but real." United States v. Hilton, 363 F.3d 58, 64 (1st Cir. 2004).

The actions taken by the OAG when it sought a court order demonstrate that the OAG understood the kind of evidence a court would require before suppression of presumptively protected material. The OAG consulted a doctor before obtaining the only court order issued under the Act to make certain the images subject to the order were child pornography. Defendant did not take any such precautions before issuing Informal Notices. FOF ¶ 88.

The Supreme Court's opinion in Ashcroft undercuts the Camfield court's assertion that an obscenity determination is more difficult than a child pornography determination. Based on the Court's guidance in Ashcroft and the measures taken by the OAG, this Court cannot conclude that fewer procedural protections are necessary before child pornography is removed from

circulation than those that are required for obscenity. Moreover, even if fewer protections were necessary, the ex parte, probable cause determination provided for in the Act is insufficient.

3. Informal Notices

Defendant argues that the Informal Notice process is not subject to constitutional scrutiny because it is informal and not coercive. Def.'s Supp. Mem. at 56-57. In Bantam Books, the Supreme Court was careful to note that all informal contacts between law enforcement and distributors of material protected by the First Amendment are proscribed. According to the Court, "We do not hold that law enforcement officers must renounce all informal contacts with persons suspected of violating valid laws prohibiting obscenity. Where such consultation is genuinely undertaken with the purpose of aiding the distributor to comply with such laws and avoid prosecution under them, it need not retard the full enjoyment of First Amendment freedoms." Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 71-72 (1963).

The Court begins by noting that an informal process cannot be used to effectuate an unconstitutional Act. Thus, because the Court concludes that the Act is unconstitutional, defendant will be enjoined from sending Informal Notices pursuant to the Act. However, even if the Court had upheld the Act, the Informal Notice process would not have survived First Amendment scrutiny for several reasons. First, the Informal Notice process provides even less procedural protection than the statutory system because the determination of pornography is made by law enforcement officials, not a judge. Second, the Informal Notice system is closer to the system of state censorship found unconstitutional in Bantam Books than the "informal contacts" permitted by that case. The notices in Bantam Books were sent by an administrative agency and circulated to law enforcement agencies. Id. at 63. The Informal Notices were more

coercive because they were sent by law enforcement officials. The Notices did more than inform ISPs that child pornography had been accessed on their service. The Notices informed ISPs that they "must" or "should" disable access to the alleged child pornography. FOF ¶¶ 71-73. This language is much more coercive than the request for "cooperation" found objectionable in Bantam Books. Bantam Books, 372 U.S. at 62. Finally, like the letters in Bantam Books, the final form of the Informal Notice informed ISPs that defendant would seek a court order if the ISP failed to comply. FOF ¶ 73.

In Bantam Books, the Supreme Court rejected an argument similar to defendant's argument that the book distributors were free to disregard letters from the Rhode Island Commission. According to the Court, a distributor was "'free' to ignore the Commission's notices, in the sense that his refusal to 'cooperate' would have violated no law. But it was found as a fact [that] compliance with the Commission's directives was not voluntary. People do not lightly disregard public officers' thinly veiled threats to institute criminal proceedings against them if they do not come around." Id. at 68. Similarly, the evidence establishes that ISPs did not view compliance with the Informal Notices as voluntary. FOF ¶ 83. In fact, all but one ISP complied with the Informal Notices. FOF ¶ 94. In the one instance when an ISP, WorldCom did not respond to Informal Notices, defendant carried out its "thinly veiled threat" and obtained a court order against WorldCom and subsequently issued a press release describing the legal proceeding. FOF ¶¶ 84-91. Based on the evidence presented, compliance with the Informal Notices was not voluntary and the Informal Notice process resulted in a prior restraint on protected expression.

D. INTERSTATE COMMERCE CLAUSE

Plaintiffs argue that the Act and Informal Notices violate the Commerce Clause because,

given the fact that most ISP's networks cross state boundaries, the blocking orders "impose restrictions on communications occurring wholly outside of a Pennsylvania, effect an impermissible burden on interstate commerce, and risk subjecting Internet speech to inconsistent state obligations." Pls. Mot. at 58.

The Constitution grants Congress the power "to regulate Commerce . . . among the several States." U.S. Const. art. I, § 8, cl. 3. The Supreme Court has decided that the Commerce Clause has a negative aspect, commonly called "the dormant Commerce Clause," that limits the states' power to regulate interstate commerce. "The dormant Commerce Clause prohibits the states from imposing restrictions that benefit in-state economic interests at out-of-state interests' expense." Cloverland-Green Spring Dairies, Inc. v. Pa. Milk Mktg. Bd., 298 F.3d 201, 210 (3d Cir. 2002) (citing West Lynn Creamery, Inc. v. Healy, 512 U.S. 186, 192-93 (1994)).

The first question the Court must answer in conducting a dormant Commerce Clause analysis is "whether the state regulation at issue discriminates against interstate commerce 'either on its face or in practical effect.' If so, heightened scrutiny applies." Id. "On the other hand, if the state regulation does not discriminate against interstate commerce, but 'regulates even-handedly' and merely 'incidentally' burdens it, the regulation will be upheld unless the burden is 'clearly excessive in relation to the putative local benefits.'" Id. at 211 (quoting Pike v. Bruce Church, Inc. 397 U.S. 137, 142 (1970)).

Plaintiffs do not argue that the Act favors in-state commerce over out-of-state commerce on its face or in practical effect. As a result, the balancing test applied in Pike v. Bruce Church quoted above will be applied. Plaintiffs also argue that a Act is per se invalid under the dormant Commerce Clause because it has the "practical effect" of regulating commerce occurring wholly

outside state's borders. Pls.' Mot. at 58 (quoting Healy v. Beer Institute Inc., 491 US 324, 336 (1989)).

1. Pike Balancing Test

The Act cannot survive the dormant Commerce Clause balancing test set forth in Pike v. Bruce Church, Inc. 397 U.S. 137 (1970). Under Pike, if the Act is an "[e]venhanded regulation to effectuate a legitimate local public interest, and its effects on interstate commerce are only incidental, it will be upheld unless the burden imposed is clearly excessive in relation to local benefits." Id. at 142. In this case, there is a legitimate local interest – combating child pornography and sexual abuse of children – and the effects on interstate commerce are only incidental. Thus, the Court must determine if the burden imposed is clearly excessive in relation to local benefits.

The courts in PSInet, Johnson, and Pataki concluded that the burdens of state pornography laws were clearly excessive in relation to local benefits. PSInet, 362 F.3d at 240, ACLU v. Johnson, 194 F.3d at 1160-61, Pataki, 969 F. Supp. at 177-181. In fact, every federal court that examined a state law that directly regulated the Internet determined that the state law failed the Pike balancing test. Id.; but see Ford Motor Co. v. Tex. DOT, 264 F.3d 493, 505 (5th Cir. 2001) (distinguishing "incidental regulation of internet activities" in that case from direct regulation in Pataki).

This Court also concludes that the burdens imposed by the Act are clearly excessive in relation to the local benefits. Defendant claims the Act is justified by reducing the sexual abuse of children. However, as discussed, defendant did not produce any evidence that the Act effectuates this goal. See supra § IV.B.2. To the contrary, there have been no prosecutions of child

pornographers and the evidence shows that individuals interested in obtaining or providing child pornography can evade blocking efforts using a number of different methods. Id.

Moreover, there is evidence that this Act places a substantial burden on interstate commerce. Defendant argues that the Act only burdens child pornography, which is not a legitimate form of commerce. To the contrary, the evidence demonstrates that implementation of the Act has impacted a number of entities involved in the commerce of the Internet – ISPs, web publishers, and users of the Internet. To comply with the Act, ISPs have used two types of filtering – IP filtering and DNS filtering – to disable access to alleged child pornography. This filtering resulted in the suppression of 376 web sites containing child pornography, certainly a local benefit. However, the filtering used by the ISPs also resulted in the suppression of in excess of 1,190,000 web sites not targeted by defendant and, as demonstrated at trial, a number of these web sites, probably most of them, do not contain child pornography. FOF ¶¶ 164-189. The overblocking harms web publishers which seek wide distribution for their web sites and Internet users who want access to the broadest range of content possible. For example, as a result of a block implemented by AOL in response to an Informal Notice, Ms. Goldwater, a self employed documentary film maker, was unable to access a web site selling movie posters. FOF ¶ 98; Tr. 1/28/04 (Goldwater) pp. 111, 121.

Based on this evidence, the Court concludes that the burden imposed by the Act is clearly excessive in relation to the local benefits. Thus, the Act must fail under the dormant Commerce Clause as an invalid indirect regulation of interstate commerce.

2. Per se Invalidity

A number of cases have invalidated state laws regulating the Internet because the laws

regulated activity occurring wholly outside the state's borders or because they have had an "extraterritorial" effect. The court in American Libraries Ass'n v. Pataki, 969 F. Supp. 160, 177 (S.D.N.Y. 1997) invalidated a New York state law that regulated the Internet because "[t]he nature of the Internet makes it impossible to restrict the effects of the New York Act to conduct occurring within New York. . . . Thus, conduct that may be legal in the state in which the user acts can subject the user to prosecution in New York and thus subordinate the user's home state's policy – perhaps favoring freedom of expression over a more protective stance – to New York's local concerns." This ruling was followed in American Booksellers Foundation v. Dean, 342 F.3d 96 (2d Cir. 2003), ACLU v. Johnson, 194 F.3d 1149, 1161 (10th Cir. 1999), and cited with approval in PSInet v. Chapman, 362 F.3d 227 (4th Cir. 2004). As explained in Healy v. The Beer Institute, 491 U.S. 324 (1989), the Commerce Clause protects against "against inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another State." Id. at 337.

This Act has the practical effect of exporting Pennsylvania's domestic policies. Pataki, 969 F. Supp. at 174. As an example, a WorldCom witness testified that a customer in Minnesota would not be able to access a web site hosted in Georgia if an IP Address was blocked by a Pennsylvania order. FOF ¶ 210-215. The Act is even more burdensome than the legislation examined in Pataki because Pennsylvania has suppressed speech that was not targeted by the Act. Thus, a Minnesotan would be prevented from accessing a Georgia web site that is not even alleged to contain child pornography.

A number of courts have concluded that the Internet should not be subject to state regulation. Am. Booksellers Found. v. Dean, 342 F.3d 96, 104 (2d Cir. 2003) ("We think it likely

that the internet will soon be seen as falling within the class of subjects that are protected from State regulation because they 'imperatively demand[] a single uniform rule.'"), American Libraries Ass'n v. Pataki, 969 F. Supp. 160, 181 (S.D.N.Y 1997) ("The courts have long recognized that certain types of commerce demand consistent treatment and are therefore susceptible to regulation only on a national level. The Internet represents one of those areas; effective regulation will require national, and more likely global, cooperation. Regulation by any single state can only result in chaos, because at least some states will likely enact laws subjecting Internet users to conflicting obligations."). Although the Court is not prepared to rule that states can never regulate the Internet, the Act's extraterritorial effect violates the dormant Commerce Clause.

V. CONCLUSION

For the foregoing reasons, plaintiffs' Motion for Declaratory Relief and Preliminary and Permanent Injunctive Relief is granted. Pennsylvania's Internet Child Pornography Act, 18 Pa. Stat. Ann. § 7621-7630 and the Informal Notice process used by defendant to implement the Act are declared unconstitutional. Defendant is enjoined from taking any action against an ISP for failing to comply with an Informal Notice or court order under the Act. The ISPs which blocked web sites pursuant to Informal Notices and, with respect to WorldCom, a court order shall promptly remove the blocks.

An appropriate Order follows.

APPENDIX A

PENNSYLVANIA CONSOLIDATED STATUTES

TITLE 18. CRIMES AND OFFENSES

CHAPTER 76. COMPUTER OFFENSES

SUBCHAPTER C. INTERNET CHILD PORNOGRAPHY

§ 7621. Definitions

The following words and phrases when used in this subchapter shall have the meanings given to them in this section unless the context clearly indicates otherwise:

"Child pornography." As described in section 6312 (relating to sexual abuse of children).

"Internet." The myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected worldwide network of networks that employ the transmission control protocol/Internet protocol or any predecessor or successor protocols to such protocol to communicate information of all kinds by wire or radio.

"Internet service provider." A person who provides a service that enables users to access content, information, electronic mail or other services offered over the Internet.

§ 7622. 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 section 7628 (relating to notification procedure) that child pornography items reside on or are accessible through its service.

§ 7623. Protection of privacy

Nothing in this subchapter may be construed as imposing a duty on an Internet service provider to actively monitor its service or affirmatively seek evidence of illegal activity on its service.

§ 7624. Penalty

Notwithstanding any other provision of law to the contrary, any Internet service provider who violates section 7622 (relating to duty of Internet service provider) commits:

(1) A misdemeanor of the third degree for a first offense punishable by a fine of $ 5,000.

(2) A misdemeanor of the second degree for a second offense punishable by a fine of $ 20,000.

(3) A felony of the third degree for a third or subsequent offense punishable by a fine of $ 30,000 and imprisonment for a maximum of seven years.

§ 7625. Jurisdiction for prosecution

The Attorney General shall have concurrent prosecutorial jurisdiction with the county district attorney for violations of this subchapter. No person charged with a violation of this subchapter by the Attorney General shall have standing to challenge the authority of the Attorney General to prosecute the case. If a challenge is made, the challenge shall be dismissed and no relief shall be available in the courts of this Commonwealth to the person making the challenge.

§ 7626. Application for order to remove or disable items

An application for an order of authorization to remove or disable items residing on or accessible through an Internet service provider's service shall be made to the court of common pleas having jurisdiction in writing upon the personal oath or affirmation of the Attorney General or a district attorney of the county wherein the items have been discovered and, if available, shall contain all of the following information:

(1) A statement of the authority of the applicant to make the application.

(2) A statement of the identity of the investigative or law enforcement officer that has, in the official scope of that officer's duties, discovered the child pornography items.

(3) A statement by the investigative or law enforcement officer who has knowledge of relevant information justifying the application.

(4) The Uniform Resource Locator providing access to the items.

(5) The identity of the Internet service provider used by the law enforcement officer.

(6) A showing that there is probable cause to believe that the items constitute a violation of section 6312 (relating to sexual abuse of children).

(7) A proposed order of authorization for consideration by the judge.

(8) Contact information for the Office of Attorney General, including the name, address and telephone number of any deputy or agent authorized by the Attorney General to submit notification.

(9) Additional testimony or documentary evidence in support of the application as the judge may require.

§ 7627. Order to remove or disable certain items from Internet service provider's service

Upon consideration of an application, the court may enter an order, including an ex parte order as requested, advising the Attorney General or a district attorney that the items constitute probable cause evidence of a violation of section 6312 (relating to sexual abuse of children) and that such items shall be removed or disabled from the Internet service provider's service. The court may include such other information in the order as the court deems relevant and necessary.

§ 7628. Notification procedure

(a) DUTY OF ATTORNEY GENERAL.-- The Attorney General shall have exclusive jurisdiction to notify Internet service providers under this subchapter. The Attorney General shall initiate notification under this subchapter if requested in writing by a district attorney who has provided the Attorney General with a copy of an application made under section 7626 (relating to application to remove or disable items) and a copy of the order issued under section 7627 (relating to order to remove or disable certain items from Internet service provider's service) or upon the issuance of an order based upon an application filed by the Attorney General.

(b) TIMELY NOTIFICATION.-- For purposes of this section, an Internet service provider or the person designated by the Internet service provider as provided for in section 7629 (relating to designated agent) shall be notified in writing by the Attorney General within three business days of the Attorney General's receipt of an order.

(c) CONTENTS.-- The notice shall include the following information:

(1) A copy of the application made under section 7626.

(2) A copy of the court order issued under section 7627.

(3) Notification that the Internet service provider must remove or disable the item

residing on or accessible through its service within five business days of the date of receipt of the notification.

(4) Contact information for the Office of Attorney General, including the name, address and telephone number of any deputy or agent authorized by the Attorney General to submit notification pursuant to this subsection.

§ 7629. Designated agent

An Internet service provider may designate an agent to receive notification provided under section 7628 (relating to notification procedure).

§ 7630. Report to General Assembly

The Attorney General shall make an annual report to the chairman and minority chairman of the Judiciary Committee of the Senate and to the chairman and minority chairman of the Judiciary Committee of the House of Representatives providing information on the number of notifications issued and the prosecutions made under this subchapter and making any recommendations for amendatory language.

APPENDIX B

PENNSYLVANIA CONSOLIDATED STATUTES

TITLE 18. CRIMES AND OFFENSES

CHAPTER 63. MINORS

§ 6312. Sexual abuse of children

(a) DEFINITION.-- As used in this section, "prohibited sexual act" means 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.

(b) PHOTOGRAPHING, VIDEOTAPING, DEPICTING ON COMPUTER OR FILMING SEXUAL ACTS.-- Any person who causes or knowingly permits a child under the age of 18 years to engage in a prohibited sexual act or in the simulation of such act is guilty of a felony of the second degree if such person knows, has reason to know or intends that such act may be photographed, videotaped, depicted on computer or filmed. Any person who knowingly photographs, videotapes, depicts on computer or films a child under the age of 18 years engaging in a prohibited sexual act or in the simulation of such an act is guilty of a felony of the second degree.

(c) DISSEMINATION OF PHOTOGRAPHS, VIDEOTAPES, COMPUTER DEPICTIONS AND FILMS.--

(1) Any person who knowingly sells, distributes, delivers, disseminates, transfers, displays or exhibits to others, or who possesses for the purpose of sale, distribution, delivery, dissemination, transfer, display or exhibition to others, any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of 18 years engaging in a prohibited sexual act or in the simulation of such act commits an offense.

(2) A first offense under this subsection is a felony of the third degree, and a second or subsequent offense under this subsection is a felony of the second degree.

(d) POSSESSION OF CHILD PORNOGRAPHY.--

(1) Any person who knowingly possesses or controls any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of 18 years engaging in a prohibited sexual act or in the simulation of such act commits an offense.

(2) A first offense under this subsection is a felony of the third degree, and a second or subsequent offense under this subsection is a felony of the second degree.

(e) EVIDENCE OF AGE.-- In the event a person involved in a prohibited sexual act is alleged to be a child under the age of 18 years, competent expert testimony shall be sufficient to establish the age of said person.

(E.1) MISTAKE AS TO AGE.-- Under subsection (b) only, it is no defense that the defendant did not know the age of the child. Neither a misrepresentation of age by the child nor a bona fide belief that the person is over the specified age shall be a defense.

(f) EXCEPTIONS.-- This section does not apply to any material that is possessed, controlled, brought or caused to be brought into this Commonwealth, or presented for a bona fide educational, scientific, governmental or judicial purpose.