UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

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

      Plaintiffs,

v.   No. 03-5051

GERALD J. PAPPERT, Attorney General of the
      Commonwealth of Pennsylvania,

      Defendant.

PLAINTIFFS' POST-TRIAL
PROPOSED FINDINGS OF FACT

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

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

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

Dated: April 9, 2004

TABLE OF CONTENTS

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

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

      Plaintiffs,

v.   No. 03-5051

GERALD J. PAPPERT, Attorney General of the
      Commonwealth of Pennsylvania,

      Defendant.

PLAINTIFFS' POST-TRIAL
PROPOSED FINDINGS OF FACT

Plaintiffs hereby respectfully submit their Post-Trial Proposed Findings of Fact,

reflecting all of the documents and testimony accepted into evidence at the hearing on Plaintiffs'

Motion for Preliminary and Permanent Injunction Relief. Plaintiffs are separately submitting

their Revised Proposed Conclusions of Law, which reference both the relevant facts below and

the applicable sections of Plaintiffs' legal briefs.

Format of Citations to the Record

Citations to the record will use the following codes:

Jt.Stip.	Joint Stipulations of Fact
Jt.Exh.	Joint Exhibit
P.Exh.	Plaintiffs' Exhibit
D.Exh.	Defendant's Exhibit
Tr. 1/6/04 p.37 (J.Smith)	Trial Transcript of 1/6/04x date at page 37 (J.Smith testimony)
Dep. of J.Smith (ISP.net)	Deposition of John Smith (of ISP named ISP.net)

Plaintiffs note that the following Proposed Findings of Fact contain – verbatim (with

internal references supplemented) – the parties' Joint Stipulations 1-58. Stipulations 59 & 60,

1

which are more explanatory in nature concerning P.Exh. 79 and Jt.Exh. 9, are not included in full.

Plaintiffs note that a number of Uniform Resource Locators ("URLs") have been redacted pursuant to the Court's Protective Orders of September 12, 2003, and February 19, 2004. A key to the redacted URLs is being filed herewith in a document entitled "Translation Key to Redacted URLs Referenced in Plaintiffs' Post-Trial Proposed Findings of Fact."

Identification of Witnesses Who Presented Evidence Through Live Testimony, Deposition Testimony, and Sworn Verification

To assist with the identification of witnesses referenced in Plaintiffs' Proposed Findings of Fact, Plaintiffs identify below all witnesses who – in person, through deposition, or through sworn verification – presented testimony to the Court:

Victim of blocking:

- **Laura Blain,** Webmaster for the Sheshequin-Ulster Community Center and the Pennsylvania Hinterland Cyber Charter School, both based in Ulster, Pennsylvania. Trial Transcript, Jan. 6, 2004.

Plaintiffs' Expert Witnesses:

- **Professor Mitchell Marcus,** former Chair of, and currently with, the Department of Computer and Information Science of the University of Pennsylvania. Trial Transcript, Jan. 6, 2004, and Feb. 26, 2004.

- **Professor Matthew Blaze,** Associate Professor with the Department of Computer and Information Science of the University of Pennsylvania. Trial Transcript, Mar. 1, 2004.

- **Michael B. Clark,** Webmaster for the Plaintiff Center for Democracy & Technology, Trial Transcript, Jan. 7, 8, 27 & 28, 2004, and Feb. 26, 2004.

Plaintiffs' Representatives, Staff Members and Board Members:

- **James Smallacombe,** owner Plaintiff PlantageNet, Inc. Trial Transcript, Jan. 7, 2004.

- **Janet Goldwater,** Member of the Board of Directors of, and member of, Plaintiff American Civil Liberties Union of Pennsylvania ("ACLU"). Trial Testimony, Jan. 28, 2004 (P.Exh. 76).

- **Gene Bishop,** Member of the Board of Directors of, and member of, Plaintiff ACLU. Sworn verification, Dec. 4, 2003 (P.Exh. 76).

- **Clark Moeller,** Member of the Board of Directors of, and member of, Plaintiff ACLU. Sworn verification, Dec. 5, 2003 (P.Exh. 76).

- **Alexander Roszko,** computer network consultant to Plaintiff ACLU. Sworn verification, Dec. 1, 2003 (P.Exh. 95).

Defendant's Expert Witness:

- **Benjamin Stern,** President, Fortress Technology, Inc., Trial Transcript, Jan. 29, 2004, Feb. 18, 2004, and Mar. 1, 2004.

Defendant's Staff Members:

- **William Ryan,** First Deputy Attorney General. Trial Transcript, Jan. 9, 2004.

- **John J. Burfete, Jr.,** Legal Counsel to the Child Sexual Exploitation Unit. Trial Transcript, Jan. 8 & 9, 2004.

- **Dennis T. Guzy, Sr.,** Supervisory Special Agent in the Child Sexual Exploitation Unit. Trial Transcript, Jan. 9, 2004.

- **Dennis J. Guzy, Jr.,** Manager of Information Resources Development, Information Technology and Law Section. Trial Transcript, Jan. 12, 2004.

ISPs' Staff Members:

- **AOL:**
  - **Christopher G. Bubb,** Assistant General Counsel of America Online. Deposition Transcript, Oct. 27, 2003.
  - **Brooke Patterson,** Senior Network Administrator. Deposition Transcript, Feb. 3, 2004.

- **Comcast:**
  - **Gary Lipscomb,** Senior Manager of Network Abuse and Policy Observance for Comcast IP Services. Deposition Transcript, Oct. 23, 2003.

- **Epix.net:**
  - **Gary Basham,** Systems Engineering Manager for Epix.net. Deposition Transcript, Oct. 22, 2003.
  - **Susan Butchko-Krisa,** in-house legal staff of Epix.net. Deposition Transcript, Oct. 22, 2003

- **Pennsylvania Online:**
  - **Michael MacDonald,** Senior Systems Administrator, Pennsylvania Online. Trial Transcript, Jan. 27, 2004.

- **Verizon:**
  - **Richard Hiester,** Manager of Verizon's IP Systems Operation. Deposition Transcript, Oct. 3, 2003.
  - **Scott Lebredo,** Senior Technology Manager for Operations for Verizon Internet Services. Deposition Transcript, Oct. 3, 2003.

- **WorldCom:**
  - **Mark Krause,** Senior Manager of Internet Infrastructure Security, WorldCom, Trial Transcript, Jan. 27, 2004.
  - **Craig Livingston Silliman,** Director of Technology and Network Legal Team for WorldCom. Deposition Transcript, Sept. 24, 2003.

Proposed Findings of Fact

1. "On February 21, 2002, Pennsylvania enacted a new statute on Internet Child Pornography, codified at 18 Pa. C.S. § 7330 and effective 60 days later (April 22, 2002) (hereafter the "Statute"). On December 16, 2002, the statute was recodified at 18 Pa. C.S. §§ 7621-7630, without change in substance. The full text of the current statute [is] submitted as Joint Exhibit 1." [Jt.Stip. 29].

2. The Statute generally permits the Defendant Pennsylvania Attorney General or any local district attorney in Pennsylvania to seek a court order to require an Internet Service Provider ("ISP") to block access by the ISP's customers to one or more specified web sites on the Internet that the Attorney General or district attorney asserts contain child pornography. 18 Pa. C.S. §§ 7627-7628.

4

3. As detailed below, in the spring of 2002 the Defendant – through his staff (hereafter the "Office of the Attorney General" or "OAG") instituted an "informal" process to enforce the Statute, and from the Spring of 2002 until September 2003, the OAG sent almost 500 "Informal Notices of Child Pornography" seeking to block access to almost 400 alleged child pornography web sites. In addition, as detailed below, in September 2002 the OAG obtained a single court order against an ISP pursuant to the Statute.

4. As detailed below, because of the technical realities of the Internet and how ISPs attempted to comply with the Informal Notices, the Statute and Informal Notices led to the short- or long-term blocking of access to a massive number of wholly innocent and lawful web sites. In all, as detailed below, more than 1.5 million innocent web sites have been blocked as a result of the Statute and the Defendant's "informal" application of the Statute.

5. On September 9, 2003, the Plaintiffs filed suit seeking to enjoin both the Informal Notice process and the application of the Statute itself, and on that date the Court entered an Order enjoining the further issuance of Informal Notices and placing limitations on the use of the Statute. [Order of Sept. 9, 2003].

6. Sections I through IV below provide important background information about the parties, the Internet, ISPs, and child pornography on the Internet. Sections V through X focus on the facts as they occurred from the passage of the Statute until the filing of this litigation. Section XI addresses various factual assertions made by the parties during the course of this case. And Sections XII and XIII relate to the relevant constitutional standards and burdens to the facts of this case.

I. The Parties

7. "All parties strongly oppose child pornography and support the prosecution of those responsible for the creation and distribution of such material." [Jt.Stip. 5].

A. Defendant Gerald Pappert

8. "The original Complaint named as the sole defendant Michael Fisher, then the Attorney General of the Commonwealth of Pennsylvania. Upon Mr. Fisher's resignation from that position on December 15, 2003, Gerald J. Pappert became Acting Attorney General and was automatically substituted as the defendant in this action. Mr. Pappert, as Acting Attorney General, has certain powers and responsibilities under the Pennsylvania statute challenged in this action, as set forth in the statute. Also, as Acting Attorney General, Mr. Pappert heads the Office of Attorney General ("OAG"), and, in his official capacity, is ultimately responsible (as Mr. Fisher's successor) for the actions of that agency regarding the Informal Notices of Child Pornography challenged in this action." [Jt.Stip. 4].

9. On February 2, 2004 (subsequent to the parties' Joint Stipulations), Mr. Pappert was sworn in as the Attorney General of Pennsylvania. *See* http://www.attorneygeneral.gov/around/pappert.cfm.

B. Plaintiffs CDT and ACLU, and Their Standing

10. "Plaintiff Center For Democracy & Technology (CDT) is a non-profit corporation incorporated under the laws of the District of Columbia, and with its principal offices 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

6

democratic values in connection with the development of the Internet. CDT sues on its own behalf." [Jt.Stip. 1].

11. Plaintiff CDT obtains its Internet access from WorldCom, which has been subject to a court order under the Statute. [P.Exh. 5 ¶ 2; Tr. 1/7/04 (M.Clark) at 183; Tr. 1/27/04 (M.Clark) at 183].

12. "Plaintiff American Civil Liberties Union of Pennsylvania (ACLU-PA) 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-PA is incorporated in Pennsylvania and has its principal place of business in Philadelphia. The ACLU sues on its own behalf, and on behalf of its members who use online communications." [Jt.Stip. 2].

13. Pennsylvania-resident members of Plaintiff ACLU obtain Internet access service from (among other ISPs) Epix.net, AOL, and Verizon. These members have occasion to utilize the "Google.com" search engine (or other search engines) to retrieve information maintained on various websites, the existence of which they have no prior knowledge. In light of that fact, each needs to have access to the broadest reaches of the Internet. [P.Exh. 76 (Verifications of Janet Goldwater, Clark Moeller and Gene Bishop].

14. Janet Goldwater, a member and board member of Plaintiff ACLU, testified that she would like to access specific web sites that are currently being blocked by the ISP she uses at her house to access the Internet, America Online, as a result of an Informal Notice. [Tr. 1/28/04 p. 113-21 (J.Goldwater)]. Specifically, Ms. Goldwater testified that she would have liked to have accessed two Spanish web sites, http://isladeesculturas.tuportal.com/page2.html and http://cazurro.tuportal.com/webs/index.html, in preparation for a recent trip to Spain and to conduct research for a documentary she is working on. [Tr. 1/28/04 p. 114-15, 120-21

(J.Goldwater)].[1] As a film maker and a movie fan, she testified that she also would be interested

in accessing a web site selling movie posters, http://www.movieposterforsale.us/afiliado8.htm.

[Tr. 1/28/04 p. 114, 121 (J.Goldwater)]. These three sites have been blocked by America Online

in response to Informal Notices 1086 and 2966. [P.Exh. 5 ¶ 6 (providing IP addresses of the

sites Ms. Goldwater wished to access); Jt.Exh. 9, Tab A, Lines 44 & 92 (listing those same IP

addresses as blocked by AOL in response to specific Informal Notices)].

C. Plaintiff PlantageNet and its Standing

15. "Plaintiff PlantageNet, Inc., is a Pennsylvania corporation incorporated under the

name "PlantagaNet, Inc." It has its principal place of business in Doylestown, PA. It has a

World Wide Web "home page" at http://www.pil.net." [Jt.Stip. 3].

16. In pretrial briefing the Defendant questioned PlantageNet's standing on a number of

theories, Def. Mem. at 10-12, most of which have effectively been repudiated by the testimony

of Defendant's own staff members. In any event, PlantageNet is certainly an ISP under the

definition of the Statute, and would certainly be at risk of receiving a blocking order if they are

permitted in the future. [*See* immediately following paragraphs].

17. PlantageNet sues on its own behalf, and on behalf of its customers who purchase

Internet access from PlantageNet and reach the Internet through such access. [Complaint ¶ 11].

18. Plaintiff PlantageNet, Inc., is an Internet Service Provider that provides to its

customers access to the Internet through dial-up, ISDN lines, or dedicated T1 connections, and

also offers hosting of web sites on the World Wide Web as well as other Internet services.

PlantageNet provides local dial-in numbers for most of the greater Philadelphia area, including

---

[1] The transcript contains typographical errors as to the precise web sites that Goldwater attempted to access.
The correct web sites are listed at P.Exh. 5 ¶ 2.

parts of New Jersey. [Tr. 1/7/04 pp.76-77, 81-83 (J.Smallacombe); P.Exh. 104, Tab 1 (screenshots from PlantageNet's web site describing services and coverage area)].

19. PlantageNet was founded as an Internet Service Provider in 1996, and currently has approximately 750 customers. For a three or four year period, PlantageNet's owner James Smallacombe was on the board of directors of a trade organization of ISPs [Tr. 1/7/04 p.70 (J.Smallacombe)]. In one online listing of Philadelphia area ISPs, PlantageNet was included as an ISP. [P.Exh. 104, Tab 2].

20. PlantageNet plainly meets the definition of "Internet Service Provider" in the Statute at issue here, in that PlantageNet "provides a service that enables users to access content, information, electronic mail or other services offered over the Internet" (quoting 18 Pennsylvania Statutes § 7621). PlantageNet provides to its users the ability to access the World Wide Web, as well as e-mail and other Internet services. [Tr. 1/7/04 pp.76-77, 104 (J.Smallacombe); P.Exh. 104, Tab 1].

21. PlantageNet "outsources" the Internet access services that it provides to most of its customers, which means that it contracts with a "wholesale" service provider – in this case one located in Maryland – to provide the dial-in modems and dedicated connections through which PlantageNet's customers access the Internet. The fact that PlantageNet's customers actually connect through another ISP is essentially invisible to the customers, who would in most cases never know that another ISP was involved. As far as PlantageNet's customers are aware, and as far as its web site would indicate, PlantageNet is the only ISP involved in providing service to the customers. [Tr. 1/7/04 pp.77-78, 107 (J.Smallacombe); P.Exh. 104, Tab 1].

22. This type of outsourcing arrangement is not uncommon for ISPs, both large and small. PlantageNet, in fact, has a customer that is itself an ISP that outsources its dial-up

services to PlantageNet. [Tr. 1/7/04 pp.78, 98-99 (J.Smallacombe)]. On the other end of the

spectrum, one of the largest ISPs in the country, Microsoft's MSN service, outsources its dial-up

services similarly to PlantageNet. [P.Exh. 13; Tr. 1/8/04 pp.44-50 (J.Burfete)]. Defendant's

expert Ben Stern terms outsourcing "a fairly common practice" and noted that many (if not most)

ISPs outsource some services. [Tr. 1/29/04 pp.70-71 (B.Stern)].

23. Notwithstanding the outsourcing arrangement under which PlantageNet offers

Internet access to it customers, the customers believe that PlantageNet is their ISP, [Tr. 1/7/04

p.125 (J.Smallacombe)], and it would appear likely that if a PlantageNet customer were to report

child pornography to the Defendant using the Defendant's web site, the customer would identify

"the company that provides your internet connection" as PlantageNet. [P.Exh. 104, Tab 4].

24. Although in pre-trial briefing the Defendant asserted that PlantageNet should not be

considered to be an ISP, Def. Mem. at 10-12, in trial testimony John Burfete, the OAG's senior

legal adviser responsible for interpretation of the Statute, stated that he would view PlantageNet

as an ISP and PlantageNet would be subject to the Statute notwithstanding the fact that it

outsourced its Internet access operations. [Tr. 1/8/04 pp.47-50 (J.Burfete)].

25. Indeed, in mid-2002 the OAG *rejected* the precise argument that Defendant

advanced against PlantageNet in its brief, when Microsoft asserted that it should not be the target

of Informal Notices because it does not own or operate its own network. OAG legal adviser

John Burfete specifically recommended that if an ISP is unable to get its third party service

providers to comply with a blocking order, the OAG should initiate legal proceedings against the

ISP. [P.Exh. 13].

26. Moreover, Special Agent Dennis Guzy Sr. – the person directly responsible for

enforcing the Statute – testified that he would view PlantageNet as an ISP subject to the Statute.

[Tr. 1/9/04 pp.125-25 (D.GuzySr.)]. Indeed, Agent Guzy specifically stated that he would

pursue a court order against PlantageNet if it were unable to comply with an Informal Notice.

[Tr. 1/9/04 pp.126-27 (D.GuzySr.)]. Although Agent Guzy said that it is unlikely that the OAG

would affirmatively subscribe to PlantageNet's services in order to enforce the Statute, Guzy

would issue an Informal Notice to PlantageNet without *any* investigation into the size and

structure of the ISP if he received a customer complaint. [Tr. 1/9/04 p.124 (D.GuzySr.)].

27. As discussed more fully below, because PlantageNet outsources the Internet access

services its customers receive, it does not control the equipment that would be necessary to

comply with a blocking order at issue in this case. [Tr. 1/7/04 pp.78-81, 97-98, 107-08

(J.Smallacombe)]. PlantageNet thus would likely be unable to comply with a blocking order,

[*id.*], and therefore would be at risk of liability under the Statute.

II. The Internet and the World Wide Web

A. The Internet is a Network of Networks

28. "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].

29. The Internet and the Web have become integral parts of our society, and are

increasingly a part of many people's day-to-day lives. [facts susceptible to judicial notice].

30. "In the United States, most people access the Internet through companies known as

Internet Service Providers ("ISPs"). Home Internet users are likely to 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 "DSL" circuit. A typical ISP's network is in turn

connected, directly or indirectly (through a larger ISP), to the network of an Internet "backbone"

11

provider (which itself typically is 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]. [*See also* Tr. 1/6/04 p.64 (M.Marcus)].

31. "Similarly, 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 greater Internet). Some businesses connect to their ISPs' 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].

32. This same basic hierarchical or "tree" structure is common throughout the Internet, including for example within the University of Pennsylvania, as explained by Plaintiffs' expert Professor Mitchell Marcus. Each academic department at the university has its own computer networks, which are in turn connected to a larger and faster (with "higher bandwidth") campus-wide network. Penn's larger network is then connected to a regional ISP, whose network is in turn connected to a very large ISP that is sometimes known as a "backbone provider." The networks of these "backbone providers" reach across the country and around the world. [Tr. 1/6/04 pp.63-64 (M.Marcus)].

33. This "network of networks" is linked together by a set of communications "protocols," which are common understandings about how communications between each network will be accomplished. The TCP/IP "suite" of protocols represent the most fundamental communications protocols on which the Internet is based. Through the use of common communications protocols, diverse (and otherwise incompatible) computers and networks can communicate with each other. [Tr. 1/6/04 pp.63, 67-68 (M.Marcus)]. "TCP/IP" stands for "Transfer Control Protocol/Internet Protocol." [P.Exh. 19, page 24].

34. A communications 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 working inside a corporation) might originate on the Internet user's computer, go to the corporation's network, then to a regional ISP's network, then to a backbone provider, then to another backbone provider, then back down to a regional ISP, then perhaps 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. [Tr. 1/6/04 pp.66-67 (M.Marcus); P.Exh. 2, page 1].

B. The Internet is a Packet-Switched Network

35. A fundamental difference between the Internet and the older telephone systems is that the historic network uses "circuit switching" while the Internet uses "packet switching." With the historic telephone network, a phone conversation connecting two telephones utilized physical wires and switches, and those wires and switches were dedicated for use in the phone call until the call terminated. [Tr. 1/6/04 p.68 (M.Marcus)].

36. In contrast to the telephone system's circuit-switched model, the Internet uses a packet-switched model, in which most physical resources (wires, switches, and other equipment) are shared by multiple simultaneous users. Almost all communications on the Internet (except very short ones) are divided into small "packets" that are separately sent over the Internet and reassembled on the receiving end. [Tr. 1/6/04 pp.68-69 (M.Marcus); Tr. 2/26/04 pp. 33-34 (M.Marcus)].

37. This use of packets can best be understood by an analogy: When mailing a document to someone, one could rip the document into small pieces, glue the pieces onto the backs of separate postcards, mail the postcards to the recipient, and then the recipient can

reassemble the cards on the other end. On the Internet, the tearing apart and reassembling of the messages are done automatically and without user intervention (or even knowledge in most cases) by the Transfer Control Protocol (TCP) portion of the TCP/IP suite of protocols. [Tr. 1/6/04 pp.68-69 (M.Marcus)].

38. The separate packets that make up a given communication on the Internet may not travel over the same path from the sender to the recipient of the communication, but may get routed within an ISP's network or in the middle of the Internet based on a variety of factors such as congestion on the network. [Tr. 1/6/04 pp.70-71 (M.Marcus)]. As Mark Krause explained,

> when you are sitting at your computer accessing a web server, the traffic for that connection . . . most of the time[] will not flow through . . . a single piece of circuitry, but might be scattered and routed through a wide range of connections across [the ISP's] network. . . . [I]f you connect to just . . . one website, there might be hundreds [or] thousands of packets that need to go to that web server, or come back from that web server. All those packets might take completely different paths to the web server and coming back from the web server.

[Tr. 1/27/04 p.50-51 (M.Krause)].

39. An overarching design principle on which the Internet is based is called the "end-to-end" model, under which the main job of the network itself is to move packets to their destination, and the main intelligence or "smarts" on the Internet would be at the end points of the network (that is, the computers sending and receiving packets). [Tr. 1/6/04 p.71 (M.Marcus)]. *See also* [Tr. 2/18/04 pp.87-90 (B.Stern) (providing a concise overview of the end-to-end principle].

C. The World Wide Web

40. "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].

41. The World Wide Web is one of the most common "applications" that are used over the Internet. The Web uses agreed-upon protocols to transmit and format web pages on web sites. The "Hypertext Transfer Protocol" ("http") controls how requests for web sites, and the web sites themselves, are transferred between computers, while the Hypertext Markup Language ("HTML") controls the formatting and layout of a web page. [Tr. 1/6/04 pp.72-73 (M.Marcus)].

42. "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].

43. To access web pages on a web site, an Internet user uses a "client" program called a "web browser." Internet Explorer and Netscape are two common web browsers. A web browser client 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. [Tr. 1/6/04 p.72-73 (M.Marcus)].

D. Domain Names and URLs

44. "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 use with his web site." [Jt.Stip. 13].

45. The right-hand-most part of a domain name (such as ".com", ".gov", or ".edu") is the broadest part, and is called the "Top Level Domain" (TLD). In the case of Professor Marcus' Information Science department "upenn.edu" is a sub-domain of the .edu TLD, and "cis.upenn.edu" is in turn a sub-domain of upenn.edu. [Tr. 1/6/04 p.76 (M.Marcus)].

46. "A domain name can be coupled with additional information to create a "Uniform Resource Locator," or "URL," which represents a more complete way to designate certain content or other resources on the Internet." [Jt.Stip. 14].

47. "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" indicates a name that can be used to locate the specific Web Server(s) that contains (or "hosts") the content for the requested Web Site. The "www" is often called the "hostname" of the Web Server, and the full www.attorneygeneral.gov is often called a "fully qualified domain name." However, the term "hostname" is often used to mean the same as "fully qualified domain name."" [Jt.Stip. 15]. [*See also* Tr. 1/6/04 pp.74-75 (M.Marcus)].

48. Although a user can often access a web site using the web site's "IP address" (as discussed more fully below), a URL is the more common method that people use to access a web site. [Tr. 1/7/04 p.5 (M.Marcus)].

49. "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 could also contain a reference to a specific "sub-page" that is contained in a web site and 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].

50. A web site's home page is effectively the default page for the web site, and by

convention is the page that a Web Server would return if no specific sub-page is specified. [Tr.

1/6/04 p.76 (M.Marcus)].

51. As an example, parsing Professor Marcus's personal home page – located at the URL

"http://www.cis.upenn.edu/~mitch/home.html" – reveals four major parts of the URL: (a) the

"http" indicates that the Hypertext Transfer Protocol should be used to retrieve the web page, (b)

"www.cis.upenn.edu" indicates the name of the Web Server that can provide the web page, (c)

"~mitch" indicates the file directory in which the web page is stored on the Web Server, and (d)

"home.html" indicates the specific page formatted with the Hypertext Markup Language to be

displayed. [Tr. 1/6/04 pp.76-77 (M.Marcus); P.Exh. 2, page 2].

52. In essence, a URL refers to the location of certain content to be retrieved, and that

content might be a web page, or possibly a specific part of a web page (such as a picture). For

example, "http://www.cis.upenn.edu/~mitch/home.html" refers to Professor Marcus's home

page, formatted in HTML. That page of HTML in turn contains a reference to the URL

"http://www.cis.upenn.edu/~mitch/marcus.jpg", which is the URL of a photograph of the

professor. ("JPG", pronounced "j-peg", is a common standard format used for pictures and other

visual images on the Web.) [Tr. 1/6/04 pp.87-88 (M.Marcus)].

53. A URL on the World Wide Web – whether pointing to a home page of HTML, a

specific sub-page of HTML, a visual image filename, or some other content – is ultimately still

only referring to *a location* where content can be found. There is nothing inherent in any URL

that refers to any specific piece of *static* content – the content is "permanent" only until the next

time it is changed by the web site's "Webmaster" (often, but not always, the owner of the web site). In other words, the actual content to which a URL points can (and often does) easily change without the URL changing in any way. [Tr. 1/6/04 p.77 (M.Marcus); Tr. 1/6/04 pp.26-28 (L.Blain)].

54. This fact is easy to see in action on an Internet web site that contains current news. For example, the URL "http://www.philly.com/mld/inquirer/news/nation/" displays the current top national news stories on the web site of the Philadelphia Inquirer newspaper. Over time the news headlines that are displayed will change, but the URL remains the same. [facts susceptible to judicial notice].

55. Thus, as a technical matter, it is impossible to identify any specific *unchanging and unchangeable* Internet content solely using a URL. At most, a URL provides only an ephemeral reference to any particular content. [*See* preceding paragraphs].

E. Browsing or Surfing the Web

56. 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:

<div align="center">

User

⬇ ⬆

User's ISP

⬇ ⬆

Internet "Backbone" Provider(s)

⬇ ⬆

Web Site's ISP

⬇ ⬆

Web Site

</div>
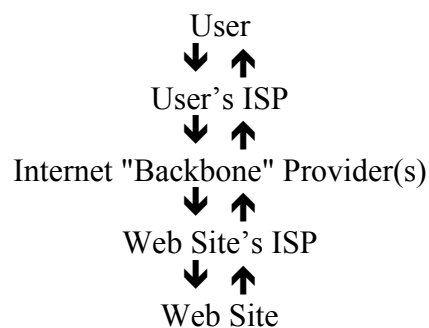
[Jt.Stip. 22].

57. To access a web page, a user can either type the URL of the web page into the user's

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 Computer and Information Science faculty

members, Professor Marcus's name would be underlined, and clicking on the name would take

the user to his personal page. [Tr. 1/6/04 pp.78-79 (M.Marcus)].

58. "In the vast majority of cases, the User's ISP is different from the Web Site's ISP."

[Jt.Stip. 23].

F. IP Addresses and the Domain Name System

59. "A URL such as http://www.attorneygeneral.gov or

http://www.geocities.com/abwlnj/homepage.html provides enough information for a human user

to access the desired web site. The user enters the URL in the user's web browser. However, the

URL alone is not sufficient for the user's computer to locate the web site. The user's computer

must first determine the numeric "Internet Protocol Address" or "IP Address" of the desired web

site. 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 computer server that can provide the desired web pages." [Jt.Stip. 24].

60. "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 and gives that address to the user's computer. This process is often called "resolving" a hostname to its IP address." [Jt.Stip. 25].

61. There are generally two types of servers involved in the IP address resolution process: recursive domain name servers and authoritative domain name servers. When a user's computer initiates a DNS request, it contacts a recursive server (commonly provided by the user's ISP or company). If the recursive server already knows the correct answer (because another user previously looked up the domain name and the recursive server stored the resulting IP address in its "cache"), the recursive server immediately returns the IP address. But if the server does not know the answer, it starts a series of requests to authoritative names servers to find the answer. For example, if a user were seeking to get to www.cis.upenn.edu, it would first ask the authoritative domain name server for the .edu domain. That authoritative domain name server would tell the recursive server how to contact the authoritative domain name server for "upenn.edu." The recursive server would then "recursively" send requests to the authoritative name servers for the "upenn.edu" domain, the "cis.upenn.edu" domain, and then finally the "www.cis.upenn.edu" domain (which would be able to return the IP address for the requested web site). [Tr. 1/6/04 pp.81-83 (M.Marcus); *see also* Tr. 1/27/04 pp.56-58. 66-67 (M.Krause) (explaining in detail the basic operation of a recursive or "caching" DNS server)].

62. "This numeric IP Address provides the user's computer with the Internet address of the Web Server to which the user's computer then sends a request for web pages with the particular URL entered in the user's web browser. IP addresses (in the most common current form) are generally expressed as a series of four numbers separated by periods, e.g., 207.102.198.176." [Jt.Stip. 26].

63. The DNS lookup process must be repeated for each separate piece of content on a web site (such as pages of HTML content, images, etc.). [Tr. 1/6/04 pp.85-88 (M.Marcus) (describing lookup process); P.Exh. 2, pages 3-5 (illustrating DNS lookup process)].

64. In the DNS lookup process described above, the user's computer must start with the IP address of the recursive domain name server to which the computer should direct DNS queries. This IP address is often provided (either manually or through an automatic setup process) by the user's ISP. [Tr. 1/6/04 pp.83-84 (M.Marcus)]. If an automated process is used, an end user may not be aware that an IP address of a DNS server has been entered into the user's computer. [Tr. 1/7/04 p.6 (M.Marcus); *see also* Tr. 1/7/04 pp.113-15 (J.Smallacombe); Tr. 1/27/04 pp.68-69 (M.Krause)].

65. Companies and other network operators, however, can choose to operate their own recursive DNS server, which is thought to speed up the process of resolving domain names to IP addresses. [Tr. 1/6/04 pp.83-84 (M.Marcus); Tr. 1/7/04 p.25 (M.Marcus)].

66. A given URL typically corresponds to only a single web site, and two different web sites cannot share the same URL. [Tr. 1/6/04 pp.89-90 (M.Marcus)].

G. The Sharing of IP Addresses

67. "Although a specific URL in general refers only to one specific web site, an individual Web Server computer can have a single IP Address and can "host" multiple different web sites. Many different web sites (each with their own different domain names) can be hosted on the same physical Web Server, and all can share the same IP Address of that Web Server." [Jt.Stip. 27].

68. "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].

69. For example, the domain name www.cis.upenn.edu (Professor Marcus's departmental web site) resolves in the DNS system to IP address 158.130.12.9. Another domain name – hlt2002.org – *also* resolves to IP address 158.130.12.9. When the Web Server located at that IP address receives an http "GET" request asking for a web page, the Server first looks at the full URL being requested to determine whether the page is from the www.cis.upenn.edu web site, or the htl2002.org web site. [Tr. 1/6/04 pp.90-92 (M.Marcus)].

70. Importantly for purposes of this case, when an http request for a particular web page is sent by the user's web browser to a Web Server, no ISP that carries the request needs to "read" the details of the request – an ISP transporting the request would only need to read the destination IP address (158.130.12.9 in the above example), and the ISP would effectively not be aware of whether the request seeks (in the above example) a web page from www.cis.upenn.edu or htl2002.org. [Tr. 1/6/04 pp.92-93 (M.Marcus)]. This fact – that an ISP carrying an http request from a web browser to a Web Server does not analyze the request itself – is consistent with the "end-to-end" model that underlies the Internet (in which the "intelligence" lies at the end points of a communication and not in the middle of the network). [Tr. 1/6/04 p.71 (M.Marcus) (discussing end-to-end model)].

71. As Professor Marcus and others have explained, the sharing of IP addresses is common on the Internet. [Tr. 1/6/04 p.94 (M.Marcus); *see also* paragraphs immediately following].

72. As detailed more fully below, it is common for web hosting companies to offer what is called "virtual web hosting," under which many web sites can be hosted on the same Web Server using the same IP address. [Tr. 1/6/04 p.94 (M.Marcus)].

73. As one small example, Plaintiff 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 pp.82-83 (J.Smallacombe)]. As another example (as discussed more fully below), Laura Blain's web site shared its IP address with more than 15,000 other domains. [Tr. 1/7/04 pp.141-42 (M.Clark)]. In a third example (also discussed below), the MyDomain.com web hosting company hosts 500,000 domains on a single IP address. [Tr. 1/8/04 pp.64-65 (J.Burfete); P.Exh. 48]. As Defendant's expert Ben Stern testified, "virtual web hosting" is "very common." [Tr. 1/29/04 p.65 (B.Stern); 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)].

74. Indeed, the OAG itself operates a number of different web sites that share the same IP address. [Tr. 1/12/04 pp.78-79 (D.GuzyJr.)].

75. One reason that it is common for IP addresses to be shared is that IP addresses are generally in short supply, and "web hosting companies" (as discussed more fully below) that need more IP addresses are strongly encouraged to share IP addresses among web sites. [Tr. 1/6/04 p.94 (M.Marcus)]. The authority responsible (in North America) for the assignment of IP addresses – the American Registry of Internet Numbers, or ARIN[2] – has proposed making the sharing of IP addresses mandatory. [Tr. 1/7/04 pp.121-22 (J.Smallacombe)]. For a brief

---

[2] Mr. Smallacombe stated that ARIN was the "Assigned Registry of Internet Numbers," Tr. 1/7/04 p.121, but ARIN is in fact the "American Registry for Internet Numbers." *See* http://www.arin.net.

explanation of the IP address assignment process as implemented by ARIN and other similar entities, *see* Tr. 1/29/04 p.37 (B.Stern).

76. Research done by Plaintiffs' expert Michael Clark empirically confirms the prevalence of shared IP addresses. Mr. Clark conducted a massive data collection and analysis of domain names and IP addresses. Using "zone files" listing all of the domain names in the leading "Top Level Domains" (.com, .net, .org, .info, .biz, .us, .aero, and .museum), Mr. Clark created a database of 29.5 million domain names and the IP addresses to which each domain named resolved. Mr. Clark collected the data in October and November of 2003, over a four-week period in which he had three computers running 24 hours a day obtaining IP addresses for each domain name. Using this database, which has been admitted into evidence in CD-ROM form as P.Exh. 77, Mr. Clark was able to analyze the frequency with which IP addresses were shared among domain names. [Tr. 1/7/04 pp.134-35, 137-40, 151-60, 170-71 (M.Clark)].

77. The raw data collected by Mr. Clark reveals that more than 90% of the 29.5 million domain names analyzed (approximately 27,040,000 million domains) share an IP address with at least one other web site, more than 75% share with at least fifty other web sites, and almost 50% share with more than 500 other web sites. [P.Exh. 79, as discussed in Jt.Stip. 59; *see also* Tr. 1/8/04 pp.3-4 (M.Clark)]. As Mr. Clark explained, the results of his research likely underrepresent the prevalence of shared IP addresses. [Tr. 1/28/04 pp.185-88 (M.Clark)].

78. In Joint Stipulation 59, the parties agreed that for a variety of reasons due to inherent limitations of the ability to collect information about all global domain names, and the phenomenon of "parking" a high number of domain names on one IP address, it is difficult to state a precise measure of how accurate the percentages are in the preceding paragraph. The

parties did agree and stipulate 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." [*See* Jt.Stip. 59].

79. With at least fifty percent of domains sharing an IP address with at least fifty other domains, and some domains sharing an IP address with thousands, tens of thousands, and even hundreds of thousands of other domains [*see* paragraphs above], the practice of shared IP addresses is a very common one affecting well over ten million domains (and probably many more).

80. One cannot easily and with any certainty determine – 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 pp.182-83 (M.Clark)]. As Mark Krause explained, it is "hard, or impossible for [an ISP] to determine what other content" might be behind a particular IP address. [Tr. 1/27/04 p.98 (M.Krause)].

H. Options for Publishing to the World Wide Web Under a Unique Domain Name, Using Various Forms of Web Hosting Services

81. "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 thus is responsible for all pages and sub-pages on a web site. Thus, "www.example.com" might 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 co-extensive with the domain name (as described above at Jt.Stip. 13 [¶ 44 above]) – is the most familiar approach to placing content on the web." [Jt.Stip. 17]. Such web sites can be published to the web using a variety of web hosting services.

82. "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 this case, a Web Publisher would contract with an ISP for Internet access, and would thereby connect the Web Server to the Internet." [Jt.Stip. 11]. [*See also* Tr. 1/6/04 p.95 (M.Marcus)].

83. "Second (and common for smaller publishers), 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 the 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. The hosting providers described at Jt.Stips. 18-20 [¶¶ 89-91 below] are a sub-category of web hosting companies." [Jt.Stip. 12].

84. Broadly defined, a "Web Host" is any company that offers a would-be 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, and include situations where, for example, a Web Hosting company provides a Web Server to service a single web site of a customer, or provides a Web Server that can be used by the customer to run multiple web sites, or provides space on a shared Web Server that services the web sites of many different customers. In many of these forms of Web Hosting, it is possible that multiple web sites are operated on a single web server using a single IP address. [Tr. 1/7/04 pp.178-81 (M.Clark)].

85. The "PlanetMike.com" web hosting company operated by the Plaintiffs' expert Mike Clark is illustrative of the diversity in Web Hosting models. PlanetMike is a customer of a Web Hosting company – Rackspace.com – that operates a Web Server that is dedicated to

PlanetMike's use. In turn, PlanetMike uses that web server to offer web hosting services to its own customers, whose web sites are then hosted together on the web server (using a single IP address). [Tr. 1/7/04 pp.179-80 (M.Clark)].

86. Web hosting where multiple web sites share a single IP address on a single Web Server is commonly called "virtual web hosting" or "name based web hosting" (so called because the Web Server serves up the requested web page based on the name of the web site being requested). Web hosting in which each web site has its own IP address is in some instances called "IP based web hosting." [Tr. 1/7/04 pp.179-80 (M.Clark)].

87. ISPs can offer a range of web hosting options. For example, Plaintiff PlantageNet offers to host the web sites of its customers. Many of PlantageNet's customers have their own domain name that they use for their web sites. [Tr. 1/7/04 pp.82-83, 100-01 (J.Smallacombe)]. Similarly, WorldCom offers (a) virtual web hosting (with hundreds or thousands of customers on a single server), (b) dedicated hosting (with one customer on a single server), (c) managed servers (where WorldCom actively manages a server for a customer), and (d) co-location space (where WorldCom provides a facility with space, power and bandwidth so that a customer can place a customer-owned server on WorldCom's premises). [Tr. 1/27/04 pp.113-15 (M.Krause)]. Pennsylvania Online offers virtual web hosting services (with many domain names on a single IP address), as well as web hosting with a single IP address for each domain name. [Tr. 1/27/04 pp.153-54 (M.MacDonald)].

I. Publishing Options Using Sub-Pages or Sub-Domains, Without Having a Wholly Unique Domain Name

88. There is, however, a range of situations in which wholly different and independent Web Publishers are responsible for different sub-pages on a single web site, or different portions of content under a single domain name. [*See* immediately following paragraphs].

27

89. "Beyond the two methods described above at Jt.Stips. 11-12 [¶¶ 82-83] Web Publishers can also publish on the World Wide Web, but 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 subpage under the provider's domain name). Thus, hypothetically, the Example Corporation might have a web site at the URL "http://www.webhostingcompany.com/example." These providers sometimes also offer their users discussion forums, chat rooms, and other services; in this case they are known more broadly as "online communities."" [Jt.Stip. 18].

90. "In the United States, for example, GeoCities is an online community, and GeoCities hosts web pages of its users. When web pages are published through an online community, the Web Publishers' web pages do not typically have their own domain name, but are sub-pages under the domain name of the online community provider. For example, 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; *see also* P.Exh. 104, Tab 5; Tr. 1/28/04 p. 24 (M.Clark)].

91. "Outside of the United States, www.terra.es is a well-known Spanish-language online community." [Jt.Stip. 20].

92. The following are examples of independent web sites hosted on Terra.es:

>   * Web site of the Bioterrorism Safety Council, at
> http://www.terra.es/personal5/safetycouncil/
>   * Web site of the ITGE Geological Survey of Spain, at
> http://www.terra.es/personal/lsomoza/marina/proyectos.html
>   * Web site of the International Philatelic Club, at
> http://www.terra.es/personal/jla31291/home.htm

[Tr. 1/28/04 pp. 25-26 (M.Clark); P.Exh. 104, Tab 9].

93. As described in Jt.Stip. 18 (¶ 89 above), "online communities" are simply one form of web hosting where a Web Publisher's web site is located on sub-pages under the domain name of the Web Host. An example of a web hosting company that offers this type of service is found at www.webspawner.com. The following are examples of independent web sites hosted on www.webspawner.com:

> * Web site of the Pennsylvania Performing Arts Academy, at
> http://www.webspawner.com/users/paperformingarts/index.html
> * Web site of a Steelton, Pennsylvania Masonic Lodge, at
> http://www.webspawner.com/users/paxton/index.html
> * Web site of a London, England, rugby football team, at
> http://www.webspawner.com/users/londonbroncos16/index.html

[Tr. 1/6/04 pp.110-14 (M.Marcus); P.Exh. 104, Tab 6; Tr. 1/28/04 p. 24 (M.Clark)].

94. "Finally, some Web Hosts allow users to create web sites using individualized "sub-domains" of the Web Hosts' primary domain. Thus, hypothetically, the Example Corporation web site might be at URL http://example.webhostingcompany.com, while another customer site might be at URL http://acehardware.webhostingcompany.com." [Jt.Stip. 20].

95. An example of a U.S.-focused Web Host that provides sub-domains to its customers is www.webalias.com. Examples of customer sites include:

> * Web site of a Western Pennsylvania web design firm, at
> http://highvoltage.andmuchmore.com/
> * Web site of an online toy store, at http://beanies.latest-info.com/

[Tr. 1/28/04 p. 24 (M.Clark); P.Exh. 104, Tab 7].

96. Many web hosting companies offer to host web sites at a very low cost, and often host those sites on a single web server using a single IP address. Other web hosting companies offer to host web sites for free in exchange for the right to put advertisements on the web site. Many small organizations use these types of low cost or free web sites to maintain a web site on

the Internet. [Tr. 1/6/04 pp. 26-30 (L.Blain) (describing creation of free and low-cost web sites for two community organizations)].

III. The Business and Operations of Internet Service Providers

97. In 2001 the U.S. government estimated that there were 8,700 Internet Service Providers in the U.S., "ranging in size from one-person operations to large organizations such as America Online and Earthlink." [P.Exh. 102, at 4].

A. ISPs Offer a Variety of Services in a Competitive Marketplace

98. From the smallest to the largest, ISPs often offer a diversity of services, including a wide range of connection speeds. Plaintiff PlantageNet, Inc., for example, provides customers access to the Internet through dial-up, ISDN lines, or dedicated T1 connections (as well as a variety of web hosting services). PlantageNet offers services primarily to customers located in parts of Pennsylvania and New Jersey. [Tr. 1/7/04 pp.76-77, 81-83 (J.Smallacombe); P.Exh. 104, Tab 1].

99. Somewhat larger but still relatively small, the ISP Pennsylvania Online provides – in central Pennsylvania – dial-up access to approximately 12,500 primarily residential customers, and web hosting services to approximately 3,000 customers. [Tr. 1/27/04 pp.126, 139-40 (M.MacDonald)].

100. At the other end of the spectrum, WorldCom, one of the largest ISPs in the world, offers Internet access service that range in speeds from dial-up access (about 56,000 bits per second) up to more than 40,000 times that speed ("OC48" speed, about 2.5 billion bits per second). WorldCom offers services in dozens of countries around the world. [Tr. 1/27/04 pp.11, 27-28, 39-40 (M.Krause)]. Like PlantageNet, WorldCom offers individual customers a choice of access methods, including dial-up and ISDN connections, as well as DSL (digital subscriber line)

access, while corporate and organizational customers might connect using T1, frame relay, ATM, or SONET technology. [Tr. 1/27/04 pp.42-43, 59, 61 (M.Krause)].

101. ISPs' networks can range in size from PlantageNet's small regional operation up to networks that operate on a national or global scale. ISP with national or larger networks are sometimes called "backbone" providers; such networks often provide Internet access service to other smaller ISPs, as well as to individuals and all sizes of businesses and organizations. [Tr. 1/27/04 pp.38-39 (M.Krause)].

102. Defendant's expert Ben Stern acknowledges that the ISP market is very competitive, and that the speed and performance of an ISP's network is an important factor in the public's perception of ISPs. [Tr. 2/18/04 p.77 (B.Stern)]. Because the market for Internet access is so competitive, an ISP's market share could certainly be harmed if complying with a blocking order in this case led to a degradation of performance. [Tr. 1/27/04 pp.136-38 (M.MacDonald)].

B. Some ISPs Outsource All or Parts of Their Operations

103. As discussed above, many ISPs "outsource" the Internet access services that they provide to their customers, which means that they contract with "wholesale" service providers to provide dial-in modems and dedicated connections to their customers. [Tr. 1/7/04 pp.77-78, 98-99 (J.Smallacombe)].

104. This type of outsourcing arrangement is common for ISPs, both large and small, ranging from very small ISPs to the Microsoft MSN service, one of the largest ISPs in the nation. [Tr. 1/7/04 pp.78, 98-99 (J.Smallacombe); P.Exh. 13; Tr. 1/8/04 pp.44-50 (J.Burfete)]. AOL, one of the largest ISPs in the world, outsources almost all of its dial-up and broadband access operations to other vendors. [Dep. of B.Patterson (AOL) at 8-9]. Similarly, Verizon outsources a significant part of its operations. [Dep. of S.Lebredo (Verizon) at 16-18, 109-10].

105. Telephone companies known as CLECs (Competitive Local Exchange Carriers) can now price wholesale Internet access so cheaply that it may be less expensive for an ISP to outsource its Internet access services. [Tr. 1/7/04 pp.98-99 (J.Smallacombe)].

106. WorldCom is also a significant wholesale provider of Internet access services, and its wholesale customers have included AOL, Earthlink, and Microsoft's MSN ISP. [Tr. 1/27/04 pp.40-41 (M.Krause)]. At the same time, WorldCom – one of the largest ISPs in the world – outsources some of the services it offers to customers (including, for example, some DSL services). [Tr. 1/27/04 pp.42-43 (M.Krause)].

C. Typical Architecture of an ISP's "Point of Presence"

107. If an ISP does not outsource all or part of its operations, it is common for the ISP to operate what is known as a "point of presence" (or "POP") through which its customers connect to the ISP's network and on to the Internet. A POP generally has (a) at least two "core" routers that "face" toward the ISP's larger network or toward the Internet, (b) a number of "edge" routers that "face" toward the ISP's customers, (c) at least two switches in between the two sets of routers, and (d) possibly a domain name server connected to one or both of the switches. This common layout is illustrated below:

Towards the ISP's core network
and through that to the Internet

Towards End Users
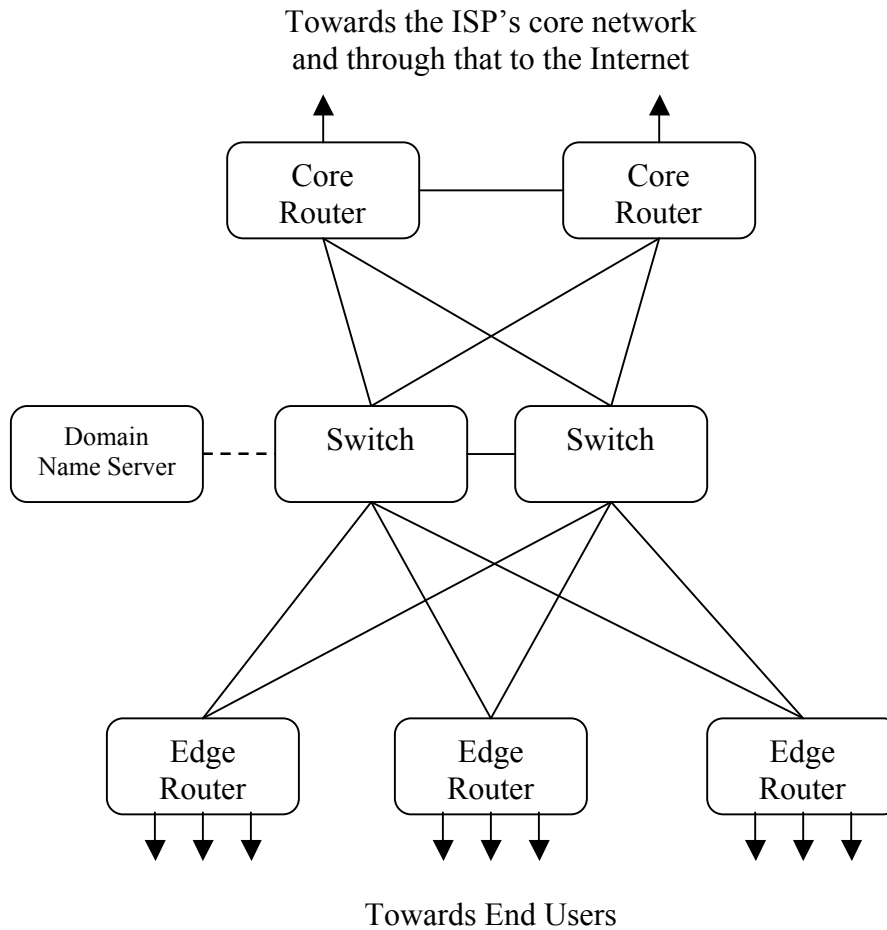
[Tr. 1/29/04 pp.40-41 (B.Stern); Tr. 1/7/04 pp.10-11 (M.Marcus); Tr. 1/27/04 pp.47-50, 71

(M.Krause)].[3] For a brief explanation of the main differences between routers and switches, see

Tr. 1/29/04 p.39 (B.Stern).

108. Although the above diagram illustrates three edge routers, some ISPs have – at

POPs in major cities – dozens or even hundreds of edge routers. Moreover, within major cities,

large ISPs may have dozens of separate physical locations that connect to customers. [Tr.

_____

[3] Plaintiffs offer this diagram to assist the Court's understanding of a common structure of a "Point of Presence," about which there was some testimony. The diagram is based on and reflects the testimony the Court received (specifically including the testimony of Defendant's expert Ben Stern), but the diagram itself was not previously submitted to the Court. The diagram, however, is very similar to a diagram reviewed by Mr. Stern in his deposition, and thus the Defendant can easily confirm the validity of this graphic rendering of the testimony. In any event, if the Defendant objects to the inclusion of this diagram as an aid to the Court, Plaintiffs would withdraw the diagram. The details of a Point of Presence are not essential to Plaintiffs' case.

1/27/04 p.53 (M.Krause)]. *See also* [Tr. 1/29/04 p.40 (B.Stern) (a POP can have a "bunch" of routers)].

109. With WorldCom's network, for example, hundreds, thousands, or even tens of thousands of customers may connect through each "edge router" (also known as a "network access point"). [Tr. 1/27/04 pp.47-48, 51-52 (M.Krause)].

110. Fundamentally, the basic goal of most ISPs' network design – the ISPs' network architecture – is to try to move traffic through the network as quickly as possible. ISPs seldom have reasons to slow the traffic down for processing, and then speed to back up. [Tr. 3/1/04 pp.146-48 (B.Stern)]

D. ISP's Attitude Toward Child Pornography and Cooperation with Law Enforcement

111. From soon after the Statute was enacted, and on numerous occasions, ISPs expressed to the OAG their desire to assist law enforcement in the battle against child pornography, and a senior official in the OAG, John Burfete, believes that the ISPs' sentiments were genuine. [Tr. 1/8/04 pp.30-31 (J.Burfete); P.Exh. 7; P.Exh. 9]. According to Mr. Burfete, the ISPs "wanted to see child pornography removed from the internet." [Tr. 1/8/04 p.38 (J.Burfete)]. The First Deputy Attorney General agreed that the ISPs did not desire to aid child pornographers. [Tr. 1/9/04 p.213 (W.Ryan)].

112. Mark Krause of WorldCom testified that his company vigorously cooperates with government and complies with court orders. [Tr. 1/27/04 pp.11-12 (M.Krause)].

113. Craig Silliman of WorldCom testified that in April 2002, soon after the Statute was enacted, ISPs made clear to the OAG that they abhor child pornography, take the issue very seriously, and dedicate significant resources to law enforcement efforts worldwide. [Dep. of C.Silliman (WorldCom) at 31-32].

114. Christopher Bubb of AOL stated in his deposition that AOL is very aggressive in its attempts to remove "any hint of child pornography" on its system, and the company is actively engaged in helping law enforcement officials with their investigations and prosecutions regarding child pornography. [Dep. of C.Bubb (AOL) at 17-18].

IV. Child Pornography and the Internet

A.   A Global Problem and a Global Law Enforcement Response

115. The parties do not dispute that child pornography is an important problem in the United States, around the world, and on the Internet. As a U.S. Government report to the Second World Congress on Commercial Sexual Exploitation of Children makes clear, since 1996 there has been a significant increase in the domestic and international focus on the problem of child pornography. Federal law enforcement actions against child pornography have significantly increased over the past eight years, as apparently has the level of international cooperation and coordination by law enforcement in the fight against child pornography. [P.Exh. 102, at 3-8].

116. The global nature of the Internet make clear the significant value in cooperation and coordination among law enforcement agencies at all levels of government, both nationally and internationally, particularly because child pornographers are "nomadic" in that they "don't stay at [web] sites very long," [Dep. of S.Lebredo (Verizon) at 45]. There is significant success in joint law enforcement efforts. For example, the Federal Bureau of Investigation's "Innocent Images National Initiative" and its Crimes Against Children Unit ("CAC") both have task forces and cooperative efforts that coordinate federal law enforcement efforts with state and local law enforcement, as well as with foreign law enforcement agencies. CAC has resources devoted to the investigation and prosecution of matters that "cross legal and geographic jurisdictional boundaries." [P.Exh. 102, at 4-5].

117. The U.S. Postal Inspection Service has major investigative operations (in conjunction with state law enforcement) focused on Internet child pornography, resulting in both federal and state criminal charges. [P.Exh. 102, at 6]. Similarly, the Cybersmuggling Center of the U.S. Customs Service works with foreign law enforcement agencies on Internet child pornography matters. One of its operations worked with law enforcement from 23 countries around the world, with substantial gathering of evidence to support both U.S. and foreign prosecutions. [*Id.* at 5]. As a Customs Official has been quoted concerning a joint U.S.-Russian operation: "One of the encouraging aspects of [the operation] was the extent to which law enforcement agencies on opposite ends of the globe worked so closely together. There really are no borders when it comes to our mutual interest in protecting children." [P.Exh. 68].

118. The U.S. Congress has specifically recognized the need for coordinated local, state, and federal law enforcement efforts to attack the problem of Internet child pornography. In 1998, Congress directed the U.S. Department of Justice to create a national network of state and local law enforcement "cyber units" to investigate Internet child sexual exploitation cases. [P.Exh. 102, at 6-7; Pub. L. No. 105–119]. According to the Department of Justice, the resulting multi-jurisdictional "Internet Crimes Against Children" ("ICAC") Task Forces help "state and local law enforcement agencies develop an effective response to cyber enticement and child pornography cases." *See* http://ojjdp.ncjrs.org/programs/ProgSummary.asp?pi=3 (official government web site of which the Court can take judicial notice).

119. It appears that as a state government, the Commonwealth of Pennsylvania has opted not to participate in the ICAC Task Force that covers Pennsylvania. According to the Task Force web site, the prosecuting authorities of Bucks, Chester, Delaware and Montgomery counties in Pennsylvania work directly with the FBI, U.S. Department of Justice, U.S. Customs

Service, and U.S. Postal Inspection Service to fight Internet child pornography. *See* http://www.delcoicac.com/links.html (official government web site of which the Court can take judicial notice). Although numerous state attorneys general and state investigative agencies participate in their ICAC Task Forces, the OAG does not appear to be significantly involved in the Pennsylvania/New Jersey/Delaware ICAC. *See* http://ojjdp.ncjrs.org/about/icac.html (listing state-by-state contacts).[4]

120. Cross-jurisdictional cooperation among law enforcement can be successful in combating Internet child pornography. For example, the U.S. Customs Service worked with state and local law enforcement agencies and foreign authorities to bring down a global child pornography web site ring based in Russia and a child pornography web site ring with ties to Denmark. [P.Exhs. 67, 68, 69]. More recently, federal agencies worked with law enforcement officials in Belarus, France and Spain to indict and arrest a Belarusian company called Regpay (and related individuals) that processed millions of dollars in credit card payments for individuals who distribute child pornography using Internet web sites. [P.Exhs. 103A, 103D[5]].

121. In the past – well before the passage of the Statute – the OAG did successfully work with both federal and local law enforcement to combat child exploitation. According to an article written by Dennis Guzy Sr., the Office "joined forces" with the U.S. Postal Inspection Service in 1997 "to formalize an already successful working relationship between state and

---

[4] This is not to suggest that the OAG is inactive in the area of child exploitation. As Dennis Guzy has explained, the OAG has been "recognized as a leading law enforcement agency . . . with respect to its proactive 'sting' operations aimed at pedophiles and child pornographers. These 'sting' operations are designed to arrest and convict those individuals who actively seek teen and pre-teen children to engage in deviate sexual conduct." [P.Exh. 65, at 2]. It appears that the OAG has chosen to devote its resources to "stings" aimed at individual pedophiles, instead of joining the ICAC or engaging in multi-jurisdictional investigations of Internet web sites.

[5] Since the submission of P.Exh. 103D, the web site of the U.S. Attorney's Office for the District of New Jersey moved, and thus the URL of P.Exh. 103D, is now http://www.usdoj.gov/usao/nj/publicaffairs/NJ_Press/files/pdffiles/regpay.indict.pdf.

federal government in an attempt to efficiently and effectively fight child pornography," and to "investigate and prosecute various sex crimes against children in cooperation with a whole host of other law enforcement agencies throughout Pennsylvania and the United States." [P.Exh. 65 at 1 (article written by Dennis Guzy Sr. and an employee of the U.S. Postal Inspection Service)]. The Office has also worked with local officials to investigate and prosecute child pornographers. [*See* P.Exh. 66 (*Commonwealth v. Pappas*, 121 Dauph. 454 (Pa. Super. Ct. 2003) (noting that Dennis Guzy Sr. "work[ed] in conjunction" with local law enforcement to investigate sexual predators of children))].

B. Methods of URL Advertisement & Distribution by Child Pornography Sites

122. As a general matter, the child pornography world can be secretive and elusive. As Special Agent Dennis Guzy has explained, some child exploitation investigative targets "closet themselves in secret groups or societies [while] [o]thers, in an effort to seek additional victims or psychological support, will often attempt to contact like-minded persons." [P.Exh. 65 at 1-2].

123. The Court has received evidence of four different methods that child pornography web sites can use to disseminate information about web sites and how to access them:

1. USENET Newsgroups and Word of Mouth

124. The Internet offers a wide range of methods for individuals to communicate with other individuals, including for example one-to-one e-mail and one-to-many "newsgroups" or "Netnews." Netnews offers tens of thousands of online discussion groups on a wide range of topics, including discussion groups focused on child pornography-related topics. [Tr. 2/26/04 pp.14-15, 28-30 (M.Marcus)].

125. Professor Blaze explained that he is familiar with underground communities on the Internet that "have a very vibrant subculture for exchanging information about the latest places to get . . . illicit, or interesting in some way, traffic. The peer-to-peer . . . music community is another example where there is direct user-to-user communications taking advantage of . . . internet bulletin boards, news groups, and . . . other techniques for exchanging data . . . ." [Tr. 3/1/04 p.33 (M.Blaze)]. "There are chat rooms and . . . private bulletin boards and private mailing lists that are available to members of the subculture that are relatively difficult to break into and join as an outsider." [Tr. 3/1/04 pp.94-95 (M.Blaze)]

126. P.Exhs. 71A and 71B are both examples of just such newsgroup postings within the child pornography subculture, in which information about accessing child pornography is disseminated. [P.Exhs. 71A & 71B]

2. "Spam" and E-Mail

127. Among the methods of dissemination of information and links to web sites available to the operators of child pornography sites is e-mail, including unsolicited "spam" e-mail. For example, the very first Informal Notice sent to WorldCom (Informal Notice 3197, sent July 1, 2002) was the result of a complaint from a citizen who received a piece of e-mail promoting a child pornography web site. [P.Exh. 26; Dep. of C.Silliman (WorldCom) at 50-51].

128. One-third of all Informal Notices sent in 2002 were the results of e-mails promoting child pornography web sites. According to the Defendant's "Annual Report to the General Assembly of Pennsylvania on the Enforcement of Act 5 of 2002," 140 of the 423 investigations that led to Informal Notices were the result of e-mails promoting the web URLs. [P.Exh. 62, at 5].

3. Advertisements on Other Web Sites and Link Sites

129. Another common technique for promoting child pornography sites is the placement of "banner" advertisements on other child pornography web sites. [*See, e.g.,* screenshots relating to Informal Notices X, Y, and Z in D.Exh. 18].

130. Indeed, as the screenshots related to Informal Notices XX and YY [*see* D.Exh. 18] demonstrate, many child pornography sites (over one hundred sites in the two examples seen) use automated web sites containing "link lists" that collect, list, and link to dozens or hundreds of child pornography sites. As explained in Informal Notice YY, the listings on the link list are fully automated and under the control of the individual web site owners. By clicking on an "Add Link" option, a web site owner can place a new child pornography URL onto the link list, thereby very quickly promulgating URLs for child pornography sites. [D.Exh. 18 (Informal Notice YY)].

131. As Professor Blaze explained, using this kind of link list, and more generally advertisements on other child pornography sites, a child pornography web site owner would be able to quickly and efficiently add or update a URL in advertising placed on web sites that are readily available to potential users of child pornography. [Tr. 3/1/04 pp.90-91 (M.Blaze)]

C. The Use of Anonymous Proxy Servers

132. A common technique for Internet users who want to keep their identity secret is the use of "anonymous proxy servers" or "anonymizers." In the context of visiting web sites, these services effectively route all http requests through the proxy server or anonymizer, which in turn sends the request to the desired web site. As a technical matter, http requests using these services outwardly appear as if they are requests directed to the service, not to the underlying URL to which the user actually seeks access. [Tr. 1/6/04 pp.132-35 (M.Marcus)].

133. Although the community of child pornography users and providers is a secretive one, there is some evidence in the record indicating that the use of anonymizers and anonymous proxy servers is encouraged for users of child pornography. One set of postings to a USENET "newsgroup," for example, suggests two child pornography sites to visit but offers the following advice:

> first make sure your browser is set up to use an anonymous proxy server because I believe the first of these sites is run by the FBI. . .
>
> If you don't use a good anonymous proxy server while surfing their site, your IP address on their logs will lead them straight to your ISP and your account there. Your IP address on their logs is evidence enough to get a search warrant for your residence. Most ISP's will gladly give them your address when they are told the police are investigating a suspected child pornography ring. . . .
>
> Get yourself a good anonymous proxyserver and go have fun at the web sites . . . .

[P.Exh. 71A]. Similarly, a "Child Pornography FAQ" ("frequently asked questions") document includes the following advice (relating most specifically to a form of Internet communications, IRC):

> Run through a proxy-server. You should always do so, anyway… It makes you totally anonymous and sometimes increases your speed on the Internet. Consult your IRC-clients manual to find out how to run through a proxy-server. A proxy-server is a computer that you connect to just like always. When you use the Internet, you're only communicating with your proxy, not the servers on the Internet. The proxy downloads everything to itself, and sends it back to you. If you have a fast proxy, the speed of your surfing should improve greatly. If it stops working, the proxy has probably been removed Just enter a new proxy, and you are back online… A great page with proxies that update often, is [URL of proxy list]

[P.Exh. 71B]. In light of these documents, it is reasonable to conclude that at least some users of child pornography use anonymizers and anonymous proxy servers (and there is no evidence in the record to the contrary).

D. Some Child Pornography is Not Self-Evident

134. Although some instances of child pornography may be readily identifiable as such, not all instances of possible child pornography prove to be illegal, and some judgments about child pornography can be difficult to make. [*See* following paragraphs.]

135. Special Agent Guzy indicated a degree of uncertainty as to whether certain content (posted by Mr. Ushakov, discussed further below) really qualified as child pornography. [Tr. 1/9/04 pp.133-34 (D.GuzySr.)].

136. In the one court action undertaken by the OAG under the Statute, the OAG did consult a physician to "make certain . . . that the materials that we saw were indeed child pornography." [Tr. 1/9/04 p.43 (J.Burfete)].

137. In *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002), the U.S. Supreme Court ruled that computer simulated images depicting children in sexual situations (but not involving the use of actual children in the creation of the images) did not constitute illegal child pornography.[6]

V. The Statute

A. Key Provisions

138. In February 2002, the Pennsylvania legislature enacted a law that imposes potential liability on Internet Service Providers for child pornography available anywhere on the Internet,

---

[6] This decision is cited here not for its legal holding, but for facts that flow from its holding – primarily the fact that a determination of whether particular images are illegal may involve facts that are not self-evident from the images themselves.

even if the ISPs are not hosting the offending content and have no relationship whatsoever with the publishers of the content. [*See* following paragraphs.]

139. The Statute requires that, upon receiving a notice from the Pennsylvania Attorney General, an ISP must within five days "disable access to" the specified content that is "accessible through its service" by customers in Pennsylvania. [18 Pa. C.S. § 7622].

140. Under the law, the Pennsylvania Attorney General or any county district attorney can apply to a local judge for an order declaring that (a) certain items on the Internet are probably child pornography under Pa. C.S. § 6312, and (b) the items shall be removed or disabled from a specified ISP's service. [18 Pa. C.S. §§ 7622, 7625-7627].

141. Section 6312 defines child pornography to include images that display, with respect to a child under the age of 18, a "lewd exhibition of the genitals or nudity if such nudity is depicted for the purpose of sexual stimulation or gratification fo any person who might view such depiction." [18 Pa. C.S. § 6312(a)].

142. The entire court proceeding can go forward on an *ex parte* basis, with no prior notice to the ISP or the web site owner required, and no post-hearing notice to the web site owner. [18 Pa. C.S. §§ 7626-7627].

143. Under the law, a judge does not make any final determination that the challenged content is child pornography; instead, the judge need only find that there is "probable cause evidence" of child pornography. [18 Pa. C.S. § 7627].

144. Once a court order is issued, the state Attorney General notifies the ISP in question. The ISP then has five days in which to block all access to the specified content, or otherwise face criminal liability, including fines up to $30,000 and a prison term of up to seven years. [18 Pa. C.S. §§ 7624, 7628].

145. As stated in the law, the location of the items in question is specified in the application to the court by its "Uniform Resource Locator." [18 Pa. C.S. § 7626(4)].

146. The Statute defines "Internet Service Provider" as "[a] person who provides a service that enables users to access content, information, electronic mail or other services offered over the Internet." [18 Pa. C.S. § 7621]. As internal documents within the OAG acknowledged, this definition of "Internet Service Provider" could encompass a very broad group of entities, including, as one OAG staff member said, "just about ALL businesses on the Internet" or at least "anyone who makes information available." [P.Exhs. 18, 38].

147. Once an order has been entered requiring that an ISP block content at a specified Internet URL, neither the judge nor the Pennsylvania Attorney General is required to withdraw the order if the challenged content changes. No entity is required to check to see if content changes, and the law makes no provision for rescinding the order. [18 Pa. C.S. §§ 7626-7628].

148. There are 67 district attorneys in the Commonwealth of Pennsylvania who could seek court orders under the Statute, and could do so without any prior consultation with or notice to the OAG. [Tr. 1/8/04 pp.28,46-47 (J.Burfete)]. From early on, the Pennsylvania District Attorneys Association (PDAA) took an active interest in the Statute; representatives of the PDAA participated in two April 2002 meetings with ISPs to discuss compliance with the Statute. [D.Exh. 3; D.Exh. 4]. Also from early on, ISPs were concerned about how the 67 district attorneys would implement the Statute. [Tr. 1/8/04 pp.109-10,119 (J.Burfete); Dep. of C.Bubb (AOL) at 207-08 (expressing concerns that district attorneys would not accept DNS filtering as compliance)]. At least one district attorney has in fact handled a complaint under the Statute (although the parties are not aware of the disposition of that matter). [Tr. 1/9/04 p.41 (J.Burfete)].

B. Goal of the Law and the OAG's Enforcement of It

149. The governmental purpose of the Statute is "[t]o protect children from sexual exploitation and abuse" and "[t]o serve this purpose by interfering with distribution of child pornography, particularly its distribution over the Internet," according to the Attorney General. [P.Exh. 75 ¶ 1].

150. According to the chief legal adviser for the OAG with regard to the Statute, the objective of the implementation of the law was "the removal of child pornography from the internet as opposed to developing criminal cases against internet service providers for . . . violation of the law." [Tr. 1/8/04 p.108 (J.Burfete)].

C. Limited Notice and Procedures

151. The Statute provides for no advance notice to anyone that a prosecutor is seeking an order, and it allows the court proceeding to go forward on an *ex parte* basis. Only the ISP against whom the order is issued is notified, and not until afterward. [18 Pa. C.S. §§ 7626-7627].

152. The lack of notice to the targeted web site and any opportunity for that web site to be heard or to defend the lawfulness of the content on the web is particularly problematic where the elements of the crime require a subjective and at times difficult judgment. [*See* Section IV.D, above].

153. When WorldCom used the IP filtering method, there was no notice provided to the web site operators whose sites would be affected. They would have no way of knowing about the block unless they noticed that overall traffic was down, researched the problem, and realized it was because they were getting no queries from a particular ISP. [Dep. of C.Silliman (WorldCom) at 148-49].

154. At least some of the web sites alleged by Defendant to contain child pornography make very strong assertions that their content is fully lawful in the United States. For example, the following statement appears on the home page of the URL http://www.RedactedURL8.com:

> This site does not contain any pornographic images. This site contains images depicting nudity. These images have been carefully reviewed by our attorneys to comply with 18 U.S.C. 2252, et seq. This law does not make nude images of minors illegal, but prohibits depictions of minors engaged in a "lascivious exhibition of the genitals or pubic area." Unlike many sites, we are based in the US and take this proscription VERY seriously. Thus you will not find any images here which violate the law. THIS SITE IS TOTALY [sic] LEGAL. All pictures of our models were taken with the presence and agreement of their parents. All content submitted on a [sic] site is a work of art. There is no age limit for work [sic] of art.

[P.Exh. 52 (HTML page from http://www.RedactedURL8.com)]. Plaintiffs have not viewed any images found on http://www.RedactedURL8.com, and offer no opinion as to whether the web site's assertion of legality is true (nor even on whether the web site is "based in the US" as asserted). Whether true or not, the prominence and strength of the assertions, made on the face of the web site, support the conclusion that the determination of unlawfulness should be made by a court of appropriate jurisdiction following an adversarial proceeding.

D. No On-Going Review of Blocked Web Sites

155. Section 7622 of the Statute requires an ISP to "remove or disable access to child pornography items residing on or accessible through its service," and Section 7626(4) requires an application for a court order to specify the "Uniform Resource Locator providing access to the items." The statute does not discuss or account for the fact that (as detailed in ¶¶ 53-55 above) a URL only provides an ephemeral reference to Internet content, and the content displayed by a given URL today may change by tomorrow. [*See* Jt.Exh. 1].

156. Specifically, the Statute lacks any provision for any subsequent or continuing review of the content located at the referenced URL to determine whether the content available there in fact continues to be child pornography. [*See* Jt.Exh. 1].

157. In practice – consistent with the Statute – the OAG did not undertake any later review to determine whether the content of a blocked URL had changed. [Tr. 1/9/04 p.97 (D.GuzySr.)]. Following the initial blocking of a site by an ISP, the only later review the OAG would conduct was 30 days later, simply to verify that the site was still blocked (not to review its content). [Tr. 1/9/04 pp.128-29 (D.GuzySr.)].

VI. The Informal Notice Process

A. Origins of the Informal Notice Process

158. From soon after the Statute was passed in February 2002, ISPs contacted the OAG to express concern about the Statute, its enforcement, and ISPs' fundamental inability to block access to content located outside of their networks. [Tr. 1/8/04 pp.27-32, 39 (J.Burfete); P.Exh. 7; P.Exh. 9].

159. 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." [Tr. 1/8/04 p.39 (J.Burfete); *see also* Dep. of C.Bubb (AOL) at 23]. The ISP's concerns specifically related to the architecture of their networks, and the fact that "based on the way that their architecture was configured, [the ISPs] could not effectively block access to websites." [Tr. 1/8/04 pp.112-13 (J.Burfete)].

160. "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

47

of the statute. On April 15, 2002, representatives of several ISPs again met with representatives

of the Attorney General, some in person, some by telephone conference call, regarding

implementation of the statute. At these meetings, the persons present discussed (1) informal

implementation of the statute 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

services." [Jt.Stip. 32].

161. Not all participants of the April 2002 meetings agree as to who first proposed the

use of an "informal" process for implementation of the Statute. [*Compare* P.Exh. 62 (OAG's

Annual Report stating that OAG "devised a method of informal compliance"); Dep. of

C.Silliman (WorldCom) at 33-34 (no agreement on informal "notices," but rather informal

cooperation); *with* Tr. 1/8/04 pp.114-15 (J.Burfete); Dep. of C.Bubb (AOL) at 33]. There is no

dispute, however, that the OAG itself had been considering the use of an informal process

independent of any proposal that may have been advanced by an ISP. [Tr. 1/8/04 p.115

(J.Burfete)]. And it is clear that following the April 2002 meetings, the ISPs did not believe that

there was any agreement on a set of procedures for implementation of the Statute. [P.Exh. 12

(April 18, 2002 letter from S.Baker to W.Ryan stating "after our most recent conference call it is

clear that we cannot arrive at such an agreement before the law takes effect")].

162. Shortly after the April meetings, on April 23, 2002, Special Agent Guzy sent an

email to representatives of several ISPs, including (among others) AOL, WorldCom and

Verizon, explaining that the Child Sexual Exploitation Unit had conducted its first successful

investigation, which is described further below. That investigation did not involve sending an

Informal Notice to or obtaining a court order against an ISP to block a web site that it did not

host. [P.Exh. 22].

163. According to John Burfete's testimony, a key justification for the informal process was that "the internet service providers wouldn't be held to a strict compliance time as they would be if we obtained formal court orders." [Tr. 1/8/04 p.116 (J.Burfete)].

164. "At the meetings in April 2002, representatives of the OAG advanced the use of "DNS filtering" (as described below) as a possible method that ISPs could use to comply with the Informal Notices." [Jt.Stip. 33].

165. The OAG did not identify *only* DNS filtering as a possible method of compliance. OAG technical staff member Dennis Guzy Jr. identified three methods of compliance: URL filtering, DNS filtering, and IP filtering. [Tr. 1/12/04 pp.16-17 (D.GuzyJr.)]. Any of those three methods would have been acceptable as a method of compliance by an ISP with a blocking order. [Tr. 1/12/04 pp.74-75 (D.GuzyJr.)].

166. The OAG's identification of possible methods of technical compliance was made 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 pp.11-12 (D.GuzyJr.)]. ISPs raised concerns that the testing was limited in scope in that it was conducted only on a "Local Area Network" (LAN) and did not accurately model a national or regional network. [Dep. of R.Hiester (Verizon) at 14; Dep. of C.Bubb (AOL) at 35].

167. As John Burfete recalled, the ISPs' response to the suggestion to use DNS filtering was to say that their technology would not allow them "to effectively comply with the statute." [Tr. 1/8/04 p.113 (J.Burfete)].

168. At no time during the April 2002 meetings did the OAG ever suggest to the ISPs that the Statute or Informal Notices could be complied with through *non*-technological means.

All means of compliance discussed were *technological* means. [Tr. 1/9/04 p.19 (J.Burfete); [Tr. 1/12/04 p.74 (D.GuzyJr.)].

169. The ISPs also raised with the OAG at those April meetings that with any method of blocking, they faced the problem of blocking non-child pornography content on the Internet. Specifically, with regard to DNS filtering it would block everything behind a given domain, and with regard to IP filtering it would block everything associated with a given IP address. (Dep. of C.Bubb (AOL) at 44-46]. Christopher Bubb of AOL, who attended the meetings, said he did not "think they were concerned by that prospect." [*Id*. at 47].

170. "On November 22, 2002, representatives of the United States Internet Service Providers Association and several ISPs met with representatives of the Office of Attorney General to discuss the statute and the informal notices." [Jt.Stip. 58]. That meeting is discussed further below.

B. Initial Two Informal Actions Pursuant to the Statute

171. The first two informal actions taken by the OAG pursuant to the Statute demonstrate how the OAG could have taken more effective steps to combat child pornography, which steps also would not have burdened speech. [*See* paragraphs immediately following].

172. Immediately after the OAG formed a special unit to implement the Statute, the OAG failed to take any direct action to prosecute an identified child pornographer. On April 22, 2002, Special Agent Dennis Guzy Sr. contacted a child pornographer the OAG had identified in Ohio, a Pavel Ushakov, and informed Mr. Ushakov that Agent Guzy had identified child pornography on his web site. Special Agent Guzy allowed him remove the pictures in question and continue his business. [P.Exh. 20, third page; Tr. 1/9/04 pp.63-67 (D.GuzySr.)]. Senior

legal adviser John Burfete confirmed on the witness stand that Agent Guzy would not have sent P.Exh. 20 unless the content was in fact child pornography. [Tr. 1/8/04 pp.52-53 (J.Burfete)].

173. Although the OAG had identified child pornography and located the person responsible for posting the content to the Internet – and that person was located one state away from Pennsylvania in Ohio – the OAG took no action to initiate criminal proceedings against Mr. Ushakov. [Tr. 1/9/04 pp.63-67 (D.GuzySr.); Tr. 1/8/04 p.54 (J.Burfete)]. The actions of the OAG did, however, lead to the removal of the child pornography from the entire Internet, and did not affect any legal web sites. [Tr. 1/8/04 p.62 (J.Burfete)].

174. In contrast, the OAG's response to the second complaint about child pornography on the Internet was far narrower in limiting access to the site in question yet potentially far more severe in its effect on innocent speech. The OAG sent an "Informal Notice" directing the Verizon ISP to block access by their customers to a child pornography site. The ISP complied, but its blocking action had no effect on the ability of the customers of any other ISP operating in Pennsylvania (or elsewhere in the world) to access the child pornography. [Tr. 1/9/04 pp.68-69 (D.GuzySr.); Tr. 1/8/04 pp.58-62 (J.Burfete); P.Exh.23]. And it had the potential, as discussed further below, to block unrelated, innocent sites.

175. As Special Agent Guzy acknowledged, the content displayed on the Internet related to the second complaint was "infinitely more horrific" than the content in the first complaint, yet the OAG allowed the content to remain on the Internet and took no action to attempt to have it removed. [Tr. 1/9/04 pp.175-77 (D.GuzySr.); P.Exh.23]. Other witnesses confirmed that going to the source of the child pornography could remove it from the entire Internet, while a blocking order to an ISP would only affect the customers of the ISP. [Tr. 1/27/04 pp.95-97 (M.Krause)].

176. This instance was certainly not the only time that the OAG decided to leave "very hard core child pornography" available on the Internet by taking no action against the web site itself (and instead simply instructing a single ISP to block access to the site). *See, e.g.,* [P.Exh. 84, 11th page (relating to Informal Notice 9162)].

C. Operation and Characteristics of the Informal Notice Process

177. To enforce the Statute, the OAG "formed a Child Sexual Exploitation Unit to which it assigned two agents and a supervisory agent. Starting in late April 2002, these agents investigated complaints by citizens regarding child pornography on the Internet and also searched the Internet on their own for child pornography using ISPs to which the OAG subscribed. As time went on, the OAG changed the ISPs to which it subscribed. The agents worked from locations in Pennsylvania." [Jt.Stip. 30].

178. Special Agent Dennis Guzy Sr. was the supervisory special agent in charge of the unit, with two agents reporting to him. [Tr. 1/9/04 p.52 (D.GuzySr.)]. Guzy has been investigating child pornography and child exploitation offenses for more than 20 years. [P.Exh. 72 (resume of D.Guzy Sr.)].

179. "The ISPs to which the OAG has subscribed at various times since April 2002 have been America Online, Verizon, WorldCom, Microsoft Network, Earthlink, Comcast, and Epix.net." [Jt.Stip. 31].

180. For the most part, following the initial startup of the Informal Notice process, at any one time, the OAG focused its Informal Notice process on only one or two ISPs at a time. A review of Jt.Exh. 9, Tab C (listing all of the Informal Notices in date order) reveals the following basic breakdown of the time frames when particular ISPs received Informal Notices:

April – mid-July 2002   Six different ISPs
Mid-July – early Nov. 2002   Verizon & AOL (including Compuserve)
Early Nov. 2002 – Feb. 2003   Earthlink & Verizon (and a few AOLs)
March – mid-May 2003   Comcast
Mid-May – Sept. 2003   Comcast & Epix.net

[Jt.Exh. 9, Tab C].

181. "Starting in late April 2002, when one of the OAG agents observed a website displaying what the agent concluded was child pornography as defined at 18 Pa. P.S. § 6312, and [Special Agent] Dennis T. Guzy reviewed the site and concurred in the conclusion, or when [Special Agent] Guzy reviewed a site identified in a citizen complaint and concluded that it displayed child pornography, an agent sent a document titled "Informal Notice of Child Pornography" to the ISP(s) 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].

182. The Informal Notices followed a standardized form, which changed somewhat over time. The first form, used from April 2002 until mid-July 2002, generally 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].

183. From mid-July 2002 through the end of 2002, the Informal Notices consolidated the first two paragraphs above and omitted the reference to Section 7330 (the statute challenged in this action), and 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 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].

184. For 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 statute challenged in this action. The Notices then 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].

54

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].

185. Although the Informal Notice language changed from a "must" to a "should," at no point did the OAG's office inform any ISPs that they did not need to comply with the Informal Notices or that the method of compliance they should use was changing. [Dep. of C.Bubb (AOL) at 215]. Throughout the entire time period, it was clearly understood that a failure to comply with an Informal Notice would result in a formal court proceeding as was brought against WorldCom in September 2002. Although the reference to the Statute was omitted in the second version of the Informal Notice, John Burfete added it back to the third version specifically because he wanted the ISPs to know what would happen if they failed to comply with an Informal Notice. [Tr. 1/8/04 p.122 (J.Burfete)].

186. Under all three versions of the Informal Notice, the ISP is obligated to deny "[a]ccess to uniform resources locator http://[redacted]." None of the forms of the Informal

Notice acknowledged or accounted for the fact that a URL is only an ephemeral reference to content on the Internet, and the content displayed at any given URL can change from day to day (or even minute to minute). [*See* Jt.Stips. 35-37, ¶¶ 182-184 above].

187. Specifically, all three forms of Informal Notice lack any provision for any subsequent or continuing review of the content located at the referenced URL to determine whether the content available at a given URL in fact continues to be child pornography. [*See* Jt.Stips. 35-37, ¶¶ 182-184 above].

188. The OAG's agent do not, and did not, conduct any subsequent or continuing review of the content located at the URLs specified in the Informal Notices to determine whether the content available at a given URL in fact continues to be child pornography. [Tr. 1/9/04 p.97 (D.GuzySr.)].

189. The vast majority of the Informal Notices issued referenced URLs that pointed to entire web sites or web pages, without referencing any specific visual image (denoted by a "jpg" at the end of the URL). Out of the approximately 376 separate URLs targeted in the Informal Notices, only 15 specified a specific image file to be blocked. [Jt.Exh. 9, Tab B, lines 1, 46, 47, 48, 221, 236, 267, 294, 418, 421, 422, 425, 432, 435, 436].

190. "The OAG's agents continued sending Informal Notices of Child Pornography to ISPs until September 9, 2003, when the Court entered its preliminary injunction. The agents sent approximately 250 Informal Notices to ISPs in 2002 and 220 in 2003." [Jt.Stip. 38].

191. "The ISPs generally responded to the Informal Notices by stating, in writing, that they had complied." [Jt.Stip. 39].

192. "Excluding notices sent directly to certain web hosting services as referenced in Jt.Stip. 57 [¶ 430 below], 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].

193. "The Informal Notices were not notices of court orders. At the times that the agents sent the Informal Notices, no court orders had been entered regarding the web sites identified in them." [Jt.Stip. 41].

194. "No court or administrative law tribunal reviewed or approved of any of the Informal Notices, or reviewed any of the content addressed in the Notices (in any proceeding known to the parties), prior to the times that the agents sent them to the ISPs." [Jt.Stip. 42].

195. "Except for one instance discussed below in September 2002, no court or administrative law tribunal reviewed or approved any of the Informal Notices, or reviewed any of the content addressed in the Notices (in any proceeding known to the parties), following to the times that the agents sent them to the ISPs." [Jt.Stip. 43].

196. In no instance did the OAG agents inform or provide notice to the targeted web site(s), whether prior to or following the sending of an Informal Notice to an ISP. [P.Exh.73 ¶¶ 1-3]. All together, approximately 494 separate Informal Notices – covering approximately 376 distinct URLs – were sent by the OAG. [Jt.Exh. 9, Tabs B, D; Jt.Stip. 60].

D. The Defendant Exerts Public and Private Pressure on ISPs to Comply with the Informal Notice Process

197. The OAG intended and expected that the ISPs would comply with the Informal Notices. The Informal Notices themselves are phrased in terms of commands that the recipients must comply with, and the Notices were backed up by express threats of further court proceedings. [*See* Jt.Stips. 35-37, ¶¶ 182-184 above].

198. AOL testified that it was explicitly "told by Mr. Ryan that the informal notice from the Attorney General had the same force and effect as a court order and that [ISPs] were obliged to comply with it as if it were a court order." [Dep. of C.Bubb (AOL) at 101].

199. From early in the OAG's internal discussions about strategies to respond to the technical and legal concerns raised by the ISPs, the OAG specifically considered how to place the ISPs in the untenable public position of appearing to defend child pornography. In response to specific constitutional concerns raised by the ISPs, OAG Chief Information Officer Peter Sand made clear that his strategy was to place the ISPs in a position of choosing between (a) complying with the Informal Notice process without complaint, or (b) being portrayed as defending child pornography. [P.Exh. 8, at 2]. This is the exact strategy that the OAG ultimately implemented against WorldCom through the press release discussed below. [Jt.Exh. 7].

200. The ISPs who received Informal Notices did view them as orders with which they must comply, and believed they faced serious adverse consequences – both legal and in terms of adverse publicity – if they did not. [Dep. of C.Bubb (AOL) at 100-03; Dep. of C.Silliman (WorldCom) at 114-17].

201. The OAG engaged in aggressive public intimidation of the one ISP, WorldCom, that did not agree to comply with an Informal Notice. In a letter dated July 25, 2002, WorldCom wrote to the Attorney General's Office to suggest that it should use the statutory procedures instead of the secret Informal Notices (and offering to assist in drafting a proposed order under the Statute). WorldCom specifically made clear 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. WorldCom also specifically stated that it would

"promptly comply with any court order (or other applicable legal process) relating to your fight against child pornography." WorldCom's letter made it crystal clear that its concern was with the Informal Notice process, and that it in no way wished to protect child pornographers. [Jt.Exh. 2].

202. In its letter, WorldCom specifically proposed to work with the OAG to draft a court order that "involves a technically feasible solution." [Jt.Exh. 2]. Nevertheless, the OAG did not consult with WorldCom, or even inform WorldCom that it was seeking a court order. [Tr. 1/8/04 pp.88-90 (J.Burfete)].

203. Notwithstanding WorldCom's strong assurances and offer of assistance, the Attorney General issued a press release accusing WorldCom of refusing to block child pornography: "WorldCom informed the Attorney General's Office that it would not deny access to the child pornography sites." [Jt.Exh. 7]. As John Burfete acknowledged, nothing in the press release made clear that WorldCom itself was not the host or creator of the child pornography, nor did the press release even hint at WorldCom's opposition to child pornography or its willingness to work with the OAG. [Tr. 1/8/04 pp.86, 90 (J.Burfete)].

204. In light of WorldCom's offer to work with the OAG if the OAG decided to seek a court order, WorldCom was "quite surprised" when out of the blue it received the court order and learned of the press release. As a result of the press release, WorldCom received many press inquiries. [Dep. of C.Silliman (WorldCom) at 65-66, 113].

205. Following the issuance of that press release, no ISP refused to follow any of the secret Informal Notices. [Dep. of C.Silliman (WorldCom) at 113-14; Jt.Exhs. 2, 7].

206. After Plaintiff CDT started raising constitutional concerns about the Informal Notice system of Defendant, a senior official in the OAG contacted a number of ISPs to pressure

them to "call off the dogs" at CDT. [Dep. of C.Bubb (AOL) at 114-17; Dep. of C.Silliman (WorldCom) at 118-21].

E.   Lack of Sufficient Technical Knowledge Within the OAG

207.   Although the staff of the OAG had good intentions, the Defendant's staff lacked sufficient technical knowledge of the operations of ISPs and the Internet to understand or sufficiently avoid the harmful impact of the Statute and Informal Notices. [*See* immediately following paragraphs].

208.   Senior OAG official John Burfete believed that the staff members from the OAG who met with the ISPs on April 4, 2002, "were not necessarily all that technically astute" and that Mr. Burfete – the senior legal adviser to the OAG concerning the Statute – had only limited "knowledge about the internet or the work of the ISPs." [Tr. 1/8/04 pp.27, 33 (J.Burfete)]. Eleven OAG staff members attended the April 4, 2002, meeting, including the OAG's two more technical staff members (Dennis Guzy, Jr. and Peter Sands), who also later participated in the April 15, 2002 meeting. [D.Exh. 3 (attendance list for April 4, 2002 meeting); D.Exh. 4 (attendance list for April 15, 2002 meeting); Tr. 1/8/04 pp.35-37 (J.Burfete) (Peter Sands is Chief Information Officer of the OAG)].

209.   The most knowledgeable OAG staff member actively involved in the technical aspects of this litigation – Dennis Guzy Jr. – had no experience within an ISP's network. [Tr. 1/12/04 pp.69-70 (D.GuzyJr.)].

210.   Mr. Guzy Jr. also provided to others within the OAG incorrect information about how easy it would be for an ISP to comply. For example, in March 2002 (before the first meetings with the ISPs), he told other OAG staff members that (a) ISPs can easily block access to "newsgroups" and (b) this "same technology is available for the web." [P.Exh. 8]. On cross

examination, however, Mr. Guzy admitted that newsgroups work on a subscription model under which it is "trivial" to unsubscribe from a particular newsgroup, but that the World Wide Web does not use a similar model and an ISP cannot "unsubscribe" from any particular web site. [Tr. 1/12/04 pp.92-94 (D.GuzyJr.); *see also* Tr. 2/26/04 pp. 28-29 (M.Marcus)]. Although it is easy to unsubscribe from newsgroups, Mr. Guzy admitted that the World Wide Web protocol (http) does not have any such built-in features. [Tr. 1/12/04 p.97 (D.GuzyJr.)].

211. The OAG staff members generally lacked any understanding of web hosting companies and the role they play in hosting content on the World Wide Web. In the OAG's internal "glossary" of Internet terms used for internal training, there is no reference to web hosting. [Tr. 1/8/04 pp.74-76 (J.Burfete); P.Exh. 19].

212. Until this litigation, Special Agent Dennis Guzy Sr. – the OAG official primarily responsible for enforcement of the Statute, and the individual responsible for trying to identify when child pornography sites were hosted by Web Hosting companies – did not understand the meaning of the term "web host." [Tr. 1/9/04 pp.89-90 (D.GuzySr.); Tr. 1/9/04 pp.13-14 (J.Burfete)]. Indeed, in discovery responses signed on November 14, 2003, the Defendant made clear that he understood the term "web host" only to apply to "online communities" such as GeoCities.com. [P.Exh. 73, pp.8-9 (response to Interrogatory 12); *see also* Tr. 1/9/04 pp.72-74 (D.GuzySr.)]. As Plaintiffs' expert Michael Clark explained, this definition is significantly underinclusive. [Tr. 1/7/04 pp.174-76 (M.Clark)].

213. Although Dennis Guzy *Jr.* had a correctly broad definition of "web host," [Tr. 1/12/04 p.32 (D.GuzyJr.)], he apparently never conveyed that understanding to his father, Special Agent Dennis Guzy Sr.

VII. The Single Court Application

214. In mid-July 2002, WorldCom received two packets of Informal Notices from the OAG, one dated July 16, 2002, and the other dated July 18, 2002. WorldCom investigated and determined it was not hosting the offending content. "On July 25, 2002, in response to [these] informal notices of child pornography that one of the OAG agents had sent it, the ISP WorldCom wrote a letter to the OAG" stating the steps it had taken. [Jt.Stip. 44; *see also* Jt.Exh. 2; Dep. of C.Silliman (WorldCom) at 54-57].

215. WorldCom attorney Craig Silliman also explained WorldCom's actions to Deputy Chief Burfete and Special Agent Guzy Sr. over the course of several conversations around the time the letter was sent. Burfete and Guzy explained to Silliman that they were acting pursuant to the portion of the Pennsylvania law that allowed orders to be sent to any ISP providing access to the sites, not just those hosting the sites, and that WorldCom was still required to comply. Mr. Silliman responded that he had significant concerns with regard to technical feasibility, as well as the fact that the Informal Notices did not follow the statutory procedures. Mr. Silliman told Deputy Chief Burfete that WorldCom frequently works with law enforcement officials and would be happy to work with the OAG to do something "that was technically feasible and was the most effective in actually combating the child pornography that they were concerned about." Mr. Silliman reiterated repeatedly that WorldCom would comply with any legal process, as long as it was technically feasible. After his last discussion with Chief Deputy Burfete, Mr. Silliman was left with the impression that Chief Deputy Burfete would contact him before issuing any court order. [Dep. of C.Silliman (WorldCom) at 58-64].

216. Until the OAG obtained the court order as described below, WorldCom had no communications with the OAG after the July 25, 2002, time frame. [Dep. of C.Silliman (WorldCom) at 65].

217. From the letter and prior communications with WorldCom, the OAG understood

that WorldCom would comply by means of 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 over-blocking would be done by court order. [Dep. of C.Silliman (WorldCom) at 69-71;

Jt.Exh. 2].

218. "In September 2002, the Attorney General filed an Application for an Order

Requiring an Internet Service Provider to Remove or Disable Access to Child Pornography in the

Court of Common Pleas of Montgomery County." [Jt.Stip. 45; *see* Jt.Exh. 3].

219. "On September 17, 2002, the Montgomery County Court entered an order *ex*

parte." [Jt.Stip. 45; *see also* Jt.Exh. 4]. The Court specifically ordered WorldCom to deny

access to five listed URLs. [Jt.Exh.4 ¶ 3]. The Court also ordered WorldCom to disable access

to the child pornography items in Attachment A of the Attorney General's Application, but did

not actually provide WorldCom with a copy of Attachment A. [Jt.Exh. 4 ¶¶ 3, 6]. Thus, at no

time did WorldCom have direct knowledge of what content the OAG had declared was child

pornography.

220. "On September 17, 2002, the OAG sent to WorldCom by e-mail and overnight mail

a covering letter signed by Chief Deputy Attorney General John J. Burfete, Jr., a Notice of the

Application and Order, a copy of the Order, and a copy of the Application." [Jt.Stip. 46; *see*

Jt.Exhs. 5, 6].

221. "On September 18, 2002, the OAG issued a press release," discussed above.

[Jt.Stip. 47; *see* Jt.Exh. 7].

222. "WorldCom informed the OAG that it had complied with the Notice by letter dated

September 23, 2002." [Jt.Stip. 48]. Specifically, WorldCom explained that for three of the

URLs, it had determined through publicly available information the hosting ISP, called the appropriate contact listed on the ISPs' web sites, and followed up by sending an email. Each of those three sites were removed by the web host. For the two that were based in the United States, the content was removed in a matter of hours; for the third, which was a large Spanish online community, "Terra.es," the content was removed within a couple of days (in large part due to time zone differences). [Jt.Exh. 8; Dep. of C.Silliman (WorldCom) at 78-88].

223. With regard to the other two sites identified in the court order, WorldCom sent emails to the web hosts but ultimately instituted a block on the associated IP addresses because it was unable to verify that the content had been taken down in time. [Dep. of C.Silliman (WorldCom) at 85-86, 89].

224. According to WorldCom's compliance letter, "in each case the service provider expressed surprise that the Office of the Attorney General had never contacted them directly regarding the site at issue." Mr. Silliman expanded on that in his testimony, explaining that the hosts indicated that they often take down offending materials at the request of law enforcement, and they did not understand why the request had been routed through WorldCom. In particular, individuals from Terra.es wished to contact the OAG directly to ensure that their entire domain would not be blocked in the future. As Mr. Silliman explained, the hosts preferred to get calls directly from the OAG because "in each case, they felt like they had processes in place to handle situations like this, and that would be the quickest way to deal with it." [Jt.Exh. 8; Dep. of C.Silliman (WorldCom) at 90-93].

225. WorldCom also instituted a process to track the IP addresses of the sites specified in the court order, so that if the IP address changed, it could change the block it had put in place. The IP addresses of the sites that WorldCom had been ordered to block changed only at two

basic time periods (including a number of rapid changes over a weekend). [Dep. of C.Silliman (WorldCom) at 97-99].

226. "Other than the one court application as to sites accessible through WorldCom, the OAG has not filed any applications for court orders under the statute." [Jt.Stip. 49].

227. "No Pennsylvania district attorney has filed any court application under the statute." [Jt.Stip. 50].

VIII. Compliance by ISPs with Statutory or Informal Notices

A. Methods of Implementation Used by ISPs

228. "According to the ISPs, on most occasions, they attempted to comply with the Informal Notices by making entries in certain equipment under their control. These entries were of two separate kinds, and were either used alone or together." [Jt.Stip. 51].

229. One "method has been variously termed "IP filtering" and "null routing."" [Jt.Stip. 54].

230. Another "method has been variously termed "DNS filtering," "DNS spoiling," and "DNS poisoning."" [Jt.Stip. 52].

231. "On occasion, ISPs have located and contacted the host of the sites identified in Informal Notices or the Notice of Court Order with the result that the hosts removed the sites from their services or servers." [Jt.Stip. 56].

1. IP Filtering

232. "With "IP filtering," an ISP first determines the IP address to which a specific URL resolves, and then can make entries in routing equipment that it controls that will stop all outgoing requests for the specific IP address." [Jt.Stip. 55].

233. As a hypothetical example, if a blocking order requires that an ISP block access to Professor Marcus's departmental web site, www.cis.upenn.edu, the ISP would make an entry into a "router" instructing the router to discard or mis-route web traffic destined for IP address 158.130.12.9. [Tr. 1/6/04 pp.97-98, 102-03 (M.Marcus)].

234. The discarding or mis-routing of an IP address is accomplished in one of two technical ways: an ISP can "null route" an IP address, or create an "access control list" (ACL). Both methods achieve the same result – Internet traffic to the IP address is blocked. [Tr. 1/7/04 p.72 (J.Smallacombe)]. Ben Stern provided a detailed explanation of the difference between null routing and using an ACL. *See* Tr. 2/18/04 pp.21-23 (B.Stern).[7]

2. DNS Filtering

235. "With "DNS filtering," an ISP can make entries in the domain name servers that it controls that will prevent requests to those servers for a specific web site's IP address from resolving to the web site's correct IP address." [Jt.Stip. 53]. [*See also* Tr. 1/29/04 pp.43-44 (B.Stern)].

B. Relative Ease of Implementation and Cost of IP and DNS Filtering

236. For many ISPs deciding how to comply with Informal Notices, IP filtering was an obvious choice because it was already in use as a standard security measure. DNS filtering was much less commonly used by ISPs for reasons other than compliance with Informal Notices, and some ISPs could not institute DNS filtering at all without substantial investment in time and money. [*See* paragraphs immediately following].

237. ISPs already have the hardware needed to implement IP filtering, and would not need to make any additional hardware investment to implement IP filtering. [Tr. 1/7/04 p.55

---

[7] Here and elsewhere in the transcript of Feb. 18, 2004, the term "null routing" is transcribed as "no routing."

(M.Marcus)]. Plaintiffs' expert Professor Matt Blaze explained that IP filtering is a "fairly routine aspect of the management of a network," and is used to respond to various types of attacks on the network, such as denial of service attacks and spam messages. [Tr. 3/1/04 pp.14-15 (M.Blaze) (explaining denial of services attacks and spam)] Mark Krause, for example, testified that IP null routing is something that WorldCom uses "routinely." [Tr. 1/27/04 pp.78-80 (M.Krause) (explaining situations in which ISPs might null route an IP address)]. Even OAG technical staff member Dennis Guzy, Jr., admitted that IP filtering is "easy to perform" and is indeed the "easiest" method for an ISP to use. [Tr. 1/12/04 pp.76-77 (D.GuzyJr.); P.Exh. 85].

238. WorldCom, for example, 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." [Tr. 1/27/04 p.52 (M.Krause)].

239. For AOL, too, 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." It is known and stable, and would not require any new equipment or have any impact on performance. (Dep. of B.Patterson (AOL) at 38-40, 52].

240. Defendant's expert Ben Stern agrees that most ISPs can implement IP filtering with their existing equipment, and many ISPs already have an existing internal procedure to implement IP-based blockage. As a general matter, the difficulty of implementation that IP filtering presents to ISPs is low. Mr. Stern also believes that the financial cost of such implementation by ISPs would be low (if any), and it would have no more than a low impact on the performance of ISPs' networks. [Tr. 2/18/04 pp.23-24 (B.Stern)].

241. In contrast, DNS filtering would not be as easily implemented by all ISPs. 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 pp.15-16 (M.Blaze)]. According to Mark Krause, DNS filtering is "not a very standard process" and "not something that ISP[s] would normally do." [Tr. 1/27/04 p.75 (M.Krause)].

242. For example, AOL has no reason to do DNS filtering for its network currently. To implement such a method today, it would have to enter the changes manually in all of its 100 DNS servers. To automate the process would entail designing a new system to do DNS filtering, assessing the related risks, assigning longterm additional staffing requirements, and developing auditing and monitoring systems, all at substantial cost. [Dep. of B.Patterson (AOL) at 47-51, 136-42]. IP filtering, on the other hand, is already in use, and is a far less risky method based on the AOL network architecture. [*Id*. at 49-51]. Given these factors, AOL network engineer Brooke Patterson said he would recommend IP filtering and would not recommend DNS filtering. [*Id*. at 51-52].

243. For WorldCom, as Mark Krause explained, DNS filtering would "require us to radically redo the way we currently implement our DNS system to our customers." [Tr. 1/27/04 pp.16-17 (M.Krause)]. According to Mr. Krause, WorldCom does not have "a built-in infrastructure to push out configuration changes to those [DNS] systems," [i*d.* 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]. [*See also id.* at 72-75 (detailing technical difficulty for WorldCom to implement DNS filtering)].

244. Mr. Krause, a senior network engineer at WorldCom, testified that he was very familiar with how WorldCom's network is set up, is involved in providing input and direction about network architectural decisions, and is involved in making decisions about what equipment to purchase within what WorldCom calls its "customer critical infrastructure." Mr. Krause has 16 years of networking experience. [Tr. 1/27/04 pp.35-36 (M.Krause)]. In addition, WorldCom attorney Craig Silliman testified that ten engineers, including those who would implement the solutions all the way up to the Senior Vice President for Internet Architecture, Vint Cerf, worked on the technical solutions for complying with a court order. [Dep. of C. Silliman (WorldCom) at 178-79]. Although Defendant's expert Ben Stern initially suggested that Mr. Krause did not sufficiently understand WorldCom's network, [Tr. 1/29/04 pp.90-92 (B.Stern)], on cross examination, Mr. Stern admitted that he was not better positioned to know what was possible or appropriate within WorldCom's network than a team of ten WorldCom engineers headed by Vint Cerf, the co-inventor of the TCP/IP protocol suite and popularly known as the "father of the Internet." [Tr. 2/18/04 pp.51-52 (B.Stern)].

245. As for cost, for ISPs that could do DNS filtering fairly easily, Defendant's expert Ben Stern acknowledges that the cost of implementing IP filtering and DNS filtering is "approximately equal." [Tr. 1/29/04 p.128 (B.Stern)] More generally, Mr. Stern would characterize the difficulty of implementation that DNS filtering presents as "low," the financial cost of DNS filtering as "low," and the performance impact of DNS filtering as "low." [Tr. 2/18/04 pp.46-47 (B.Stern)].

C. Relative Effectiveness of IP and DNS Filtering

246. IP filtering is a more effective method of complying with the Statute and Informal Notices than DNS filtering because many ISP customers do not rely on their ISP's DNS servers,

thereby rendering any DNS filtering entirely ineffective for those customers. [*See* paragraphs immediately following].

247. For many ISPs, the DNS filtering method is significantly less effective than the IP filtering method because the DNS filtering method is wholly ineffective for ISPs' customers that operate their own DNS servers. Some companies and organizations operate their own DNS servers or rely on publicly available DNS servers and thus do not use the DNS servers of their ISPs. An ISP's use of DNS filtering would have no impact on such customers. [Tr. 1/6/04 pp.115-18 (M.Marcus); P.Exh. 2, page 6 (illustrating the by-pass of a DNS filter by a company that runs its own DNS server)]. Defendant's expert Ben Stern admitted that DNS filtering is not effective with regard to ISPs' customers that do not use the DNS servers of their ISPs. [Tr. 2/18/04 p.47 (B.Stern)].[8]

248. Mr. Stern specifically acknowledged that "[l]arge businesses often operate their own [DNS servers]." [Tr. 1/29/04 pp.68-69 (B.Stern)]. And, as the following paragraphs amply confirm, a wide range of businesses and other entities operate their own DNS servers or rely on DNS servers not operated by their ISPs.

249. According to Epix.net employee Gary Basham, Epix.net customers could operate their own DNS servers or point their browsers to public DNS servers. Any DNS filtering

---

[8] Although at trial Dennis Guzy Jr. asserted that it might violate the "terms of service" for an ISP's customer to *not* use the DNS server of the ISP, [Tr. 1/12/04 p.23 (D.GuzyJr.)], no evidence of such terms of service was adduced at trial. Mr. Guzy Jr. could not identify any actual terms of service from any actual ISPs that would be violated by a customer choosing to use a DNS server other than the server provided by the ISP. [Tr. 1/12/04 pp.88-90 (D.GuzyJr.)]. Plaintiffs' expert Professor Marcus testified that he reviewed the Terms of Service for three large ISPs, AOL, Earthlink and Verizon, and none of them prohibited customers from pointing their browsers to someone else's DNS servers. In any event it would make no sense for an ISP to require its customers to use its DNS servers because if fewer people are using those DNS servers, then they need less capacity and there is less traffic through the ISP's network. [Tr. 2/26/04 pp. 23-24 (M.Marcus)]. In depositions, a number of ISPs confirmed that their terms of service would not prohibit a customer from pointing to a different DNS server. [Dep. of B.Patterson (AOL) at 143-44; Dep. of G.Lipscomb (Comcast) at 54-55; Dep. of G.Basham (Epix) at 32].

employed by Epix would be ineffective with regard to such customers. [Dep. of G.Basham (Epix) at 32-33, 41-42].

250. Senior systems administrator Michael MacDonald of the ISP Pennsylvania Online testified that it does not force people to use the ISP's DNS servers, and indeed does not know one way or another whether any particular customer uses the ISP's DNS servers. [Tr. 1/27/04 pp.145-48 (M.MacDonald)]. Pennsylvania Online would use IP filtering because it is 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*. 131-32].

251. According to senior technical engineer Mark Krause, the primary reason that WorldCom would not use DNS filtering is because "it would not allow us to fully comply with the court order . . . due to the fact that not all of our users use DNS servers under our control." [Tr. 1/27/04 p.16 (M.Krause)]. According to Mr. Krause, medium and large businesses often operate their own DNS servers. [*Id.* at 76-77].

252. In deposition, Craig Silliman of WorldCom confirmed that it did not consider DNS filtering an option because users could simply use a different DNS server. WorldCom's customer base, in particular, 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 it simply was so seriously flawed that it was not a workable solution." Mr. Silliman made that clear to the OAG. [Dep. of C.Silliman (WorldCom) at 104-06, 110-11, 133]

253. AOL expressed concerns that whatever the OAG thought of DNS filtering as a method of compliance, the 67 district attorneys empowered to enforce the Statute might not agree. [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, or, for customers not using the AOL browser, their computers might automatically rely on

non-AOL DNS servers depending on how they are accessing the AOL network. [Dep. of

B.Patterson (AOL) at 16, 44-45].

254. Verizon specifically informed the OAG that not all of its customers used its DNS

servers, and thus the DNS blocking that Verizon did would not be effective for those customers.

[Tr. 1/9/04 p.160 (D.GuzySr.); P.Exh. 84; Dep. of S.Lebredo (Verizon) at 25].

255. Indeed, even the Attorney General's own office operates its own DNS server and

thus the approximately 1,000 employees of the OAG do not rely on the DNS server of the

OAG's ISP (which happens to be Verizon). [Tr. 1/12/04 p.72 (D.GuzyJr.)]. Thus, when ISPs

told the OAG that some of the ISPs' customers would not be affected by DNS filtering, the

Office of the Attorney General had first hand knowledge that the ISPs were correct. [Tr. 1/12/04

pp.80-81, 113 (D.GuzyJr.)].

256. Rite-Aid, the company where Dennis Guzy Jr. worked before joining the OAG, also

operated its own DNS servers, [Tr. 1/12/04 p.82 (D.GuzyJr.)], and thus Rite-Aid and its

employees would be unaffected by DNS filtering.[9] Large entities such as Rite-Aid or the OAG

have automatic techniques that ensure that the computers within their networks point to the

internal DNS rather than the external public DNS system. As Dennis Guzy Jr. agreed, it is "very

---

[9] To clarify the record, in the discussion of the OAG's and Rite-Aid's operation of their own DNS servers, there are in the transcript from January 12, 2004, some significant transcription errors. Specifically, on pages 81 (line 23) and 82 (lines 12, 13, 16, 17) the word "internet" should actually be "intranet," which is effectively an inwardly-facing web server that serves content and web pages to internal users but *not* to users on the public Internet. Effectively, an "intranet" is a private and wholly internal mini-World Wide Web, and as Dennis Guzy Jr. explained, companies that have an "intranet" must also operate their own DNS servers (because the IP addresses for the internal web sites would not be listed in the public Internet's DNS system). [Tr. 1/12/04 pp.81-82 (D.GuzyJr.)].

quick" and "easy" for such entities to change the DNS servers to which the employees'

computers refer. [Tr. 1/12/04 pp.83-84 (D.GuzyJr.)].

257. Some small entities also do not use their ISPs' DNS. Plaintiff CDT, which has

fewer than 15 employees, does not use the DNS server of its ISP. In early January 2000, Mr.

Clark decided that the performance of the ISP's DNS servers was unacceptable, and so Mr. Clark

set up CDT's system to rely on its web host's DNS servers. [Tr. 1/28/04 p. 75 (M.Clark)].

258. Defendant's expert Ben Stern's experience also confirmed that a wide range of

companies choose to operate their own DNS servers. Stern's prior employer Allegiance (an ISP)

had large business customers that operated their own DNS. [Tr. 1/29/04 pp.74-75 (B.Stern)].

On the other end of the spectrum, a small company – with about five employees – that was a

client of Mr. Stern's company (Fortress Technology) also decided to operate its own DNS server.

[Tr. 2/18/04 pp.47-48 (B.Stern)].

259. IP filtering (using "null routing" or "access control lists") is highly effective in

blocking access to an IP address. [Tr. 1/7/04 pp.72-73 (J.Smallacombe)].[10]

260. Comparing IP filtering with DNS filtering, an IP filter will at the time it is

implemented be more effective than DNS filtering, because IP filtering will block all users other

than ones using anonymizing services. [Tr. 1/7/04 pp.49-50 (M.Marcus)]. Defendant's expert

Ben Stern admits that at the time they are deployed, "IP address filtering is at least as effective as

---

[10] Although a number of times throughout the trial of this case the Defendant attempted to establish that IP
address numbers were hard to remember and difficult to work with (and thus IP filtering would be less
effective because of the risk of typographical errors) [Tr. 1/7/04 pp.12-13 (M.Marcus)], the Defendant's expert
Ben Stern conceded that typographical errors were also a risk with domain names and URLs. [Tr. 2/18/04
pp.40-42 (B.Stern)]. In fact, Verizon once received an Informal Notice with a misspelled domain name to be
blocked. [Dep. of S.Lebredo (Verizon) at 63-64; Dep. of R.Hiester (Verizon) at 57-58]. The weight of the
evidence indicates that the risk of typographical errors in a URL or IP address is not great, and favors none of
the methods over any other.

DNS filtering," [Tr. 1/29/04 pp.127-28 (B.Stern)], and is "very effective" if the IP address does not change frequently, [Tr. 2/18/04 pp.31-32 (B.Stern)].

261. A child pornography web site could evade an IP filter by obtaining a new IP address for the web site. [Tr. 1/7/04 pp.14-15 (M.Marcus)]. If, however, the ISP implementing the IP filter were to monitor the web site for a new IP address, the IP filtering would remain effective. [*Id.* at 15]. Defendant's expert Ben Stern acknowledged that such a monitoring program would be easy to create. [Tr. 2/18/04 pp.33-34 (B.Stern)].

262. In fact, in the only instance of an ISP complying with a court order under the Statute, WorldCom did exactly this – it "implemented a tool to monitor for any of those [IP address] changes and to alert us to [the change], so that then we could go and adjust the null routing to follow the change made in the DNS." [Tr. 1/27/04 p.80 (M.Krause); *see also id.* at 100; Dep. of C.Silliman (WorldCom) at 97-99 (describing monitoring tool and infrequency of IP address changes)].

263. As Defendant's expert Ben Stern acknowledged, IP filtering would be effective even where (a) a user did not rely on the ISP's DNS server, (b) the web site used a non-standard port number, and (c) the web site used the secure https protocol. [Tr. 2/18/04 pp.36-39 (B.Stern)].

D. ISP's Choice Between IP Filtering and DNS Filtering

264. When faced with an Informal Notice or a court order under the Statute, many ISPs had to decide how technically to attempt to comply, and that decision generally came down to whether to implement IP filtering or DNS filtering (or both).

265. ISPs that utilized IP filtering to comply with blocking orders challenged in this case include:

- AOL [Dep. of C.Bubb (AOL) at 123-25];
- Comcast [Dep. of G.Lipscomb (Comcast) at 24-26];
- Epix.net [Dep. of G.Basham (Epix.net) at 11-14];
- Innernet.net [Jt.Exh. 9, Tab A, lines 363-66; P.Exh. 24];
- PA Online [Jt.Exh. 9,Tab A, lines 374-75; Tr. 1/27/04 pp.131 (M.MacDonald)];
- RCN Internet [Jt.Exh. 9, Tab A, line 379];
- Verizon [Dep. of S.Lebredo (Verizon) at 15-21]; and
- WorldCom [Tr. 1/27/04 pp.12-14 (M.Krause); Dep. of C.Silliman (WorldCom) at 95-98].

266. ISPs that utilized DNS filtering to comply with blocking orders challenged in this case include:

- Earthlink [Jt.Exh. 9, Tab A, lines 257-312];
- Epix.net [Dep. of G.Basham (Epix.net) at 13-18];
- RCN Internet [Jt.Exh. 9, Tab A, line 378]; and
- Verizon [Dep. of S.Lebredo (Verizon) at 15-21].

267. As seen above, a significant majority of ISPs chose to implement IP filtering, sometimes in conjunction with DNS filtering. Of the nine ISPs for which any compliance method is known, only Earthlink relied solely on DNS filtering. [*See* preceding paragraphs].

268. As detailed in the preceding two subsections, WorldCom's decision to use IP filtering instead of DNS filtering was based "primarily" on the fact that DNS filtering would be wholly ineffective for many of WorldCom's customers, and IP filtering would be easier to implement than DNS filtering. [Tr. 1/27/04 pp.16-17 (M.Krause)]. In addition, WorldCom was concerned about opening itself up to legal liability if it implemented DNS filtering because many of its customers did not use WorldCom's DNS servers. [Dep. of C.Silliman (WorldCom) at 104-11].

269. For some ISPs, DNS filtering was not a viable option as a method of compliance with an Informal Notice. When Comcast received its first Informal Notice, it attempted to apply a block at the Comcast DNS server. [Dep. of G.Lipscomb (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 felt that was inadequate. [Dep. of

G.Lipscomb (Comcast) at 21].

270. Comcast instead chose to use IP filtering as its method of compliance "because it

was most effective." [Dep. of G.Lipscomb (Comcast) at 26].

271. At least 27 of the Informal Notices specified IP addresses in the URLs. [Jt.Exh. 9,

Tab B, lines 2-9, 121-22, 125-41]. If an ISP receives a blocking order containing an IP address,

it would be unable to use DNS filtering to comply with the order, and would have to rely on IP

filtering. [Tr. 1/7/04 p. 41-42 (M.Marcus)]. Thus, any ISP that opts for DNS filtering would

also have to implement IP filtering to be able to comply with the full range of Informal Notices

sent by the OAG.

272. As a factual matter,[11] under federal law, ISPs will incur no federal or state civil

liability to any party in the event that they "overblock," thereby blocking innocent content along

with alleged child pornography content. Thus, in the face of potential criminal liability (for

blocking too little) under the Statute challenged in this action, there is no countervailing potential

civil liability (for blocking too much). [47 U.S.C. § 230(c)(2)(A)].

273. It is the official position of the OAG to refuse to tell an ISP whether any particular

method of compliance would comply with the law. [Tr. 1/8/04 pp.133-35 (J.Burfete); Tr. 1/9/04

p.178 (D.GuzySr.)].

274. Overall, the cost, internal burden, impact on performance, and minimization of legal

risk favor IP filtering over DNS filtering (excluding the fact that for effective compliance, an ISP

must implement IP filtering in any event, as discussed above). In light of the above factors, it is

---

[11] Although the interpretation of a federal statute is of course a legal question, in this context it is a factual
matter relating to the incentives and legal risks facing ISPs.

reasonable to expect that some if not most ISPs will choose to comply with Informal Notices or orders under the Statute by using the IP filtering method.

E. Some ISPs Have No Direct Ability to Comply with a Blocking Order

275. PlantageNet and other ISPs that outsource their customers' Internet access do not have any direct means to comply with an Informal Notice or Statutory blocking order. [*See* paragraphs immediately following].

276. PlantageNet has no direct technical means to comply with a blocking order. [Tr. 1/7/04 pp.80-81, 107-08 (J.Smallacombe)]. For example, although PlantageNet operates "authoritative" domain name servers, it does not for most of its customers provide the "recursive"[12] DNS service that would be necessary for DNS filtering. [*Id.* at 78-79]. Nor could PlantageNet implement IP filtering itself. [*Id.* at 97-98].

277. Similarly, a large national ISP, Microsoft's MSN, also has no direct means to comply with a blocking order. [P.Exh. 13; Tr. 1/8/04 pp.44-50 (J.Burfete)].

278. Although most AOL customer traffic passes through a data center controlled by AOL, [Dep. of B.Patterson (AOL) at 21-28], some web traffic of some AOL customers does not ever come in contact with equipment directly controlled by AOL, [*id.* at 29-31], and thus for those customers AOL has no direct means to comply with a blocking order.

279. An ISP that outsources its access service may be unable to obtain the cooperation of its wholesale providers to attempt to comply with a blocking order in this case. For example, Microsoft had significant difficulty getting its wholesale providers to cooperate, [P.Exh. 13], and

---

[12] In a number of places in the trial transcript, the word "recursive" is transcribed as "cursive." *See, e.g.,* Tr. 1/7/04 p.79. To Plaintiffs' knowledge, "cursive" is not a term that relates to DNS service, and every instance where it appears in the transcript should in fact refer to "recursive" DNS access.

only one of Verizon's two wholesale providers agreed to assist Verizon in complying with blocking orders. [Dep. of S.Lebredo (Verizon) at 29-30].

280. Similarly, although not for reasons related to this case, PlantageNet sought to have its wholesale provider direct PlantageNet's customers to PlantageNet's DNS servers (instead of the wholesale provider's), but the wholesale provider could not provide that service. [Tr. 1/7/04 pp.109-10 (J.Smallacombe)]. Although James Smallacombe testified that he might be able to ask his wholesale access provider to block access to an IP address, Mr. Smallacombe has no confidence that it would be done or would be done in a timely manner. [Tr. 1/7/04 pp.116-17 (J.Smallacombe)]. Mr. Smallacombe expressed particular concern about having to rely on the actions of another company to avoid criminal liability that would attach to PlantageNet for a failure to comply with a blocking order issued under the Statute challenged here. [Tr. 1/7/04 pp.122-23 (J.Smallacombe)].

IX. The Impact on the Internet and Protected Expression

A. Both IP Filtering and DNS Filtering Block Access to Innocent Web Sites

281. Both technical methods of compliance used by ISPs – IP filtering and DNS filtering – can and have led to the blocking of a vast number of innocent web sites. [*See* Section IX.B-C, below].

282. There is no dispute that IP filtering can lead to massive blocking of innocent web sites. As Defendant's expert Ben Stern flatly stated, IP filtering "will block innocent sites . . . a great deal," [Tr. 1/29/04 p.65 (B.Stern)], and "IP address filtering is extremely likely to block untargeted sites due to the process known as virtual hosting," [*id.* at 128]. OAG technical staff member 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. [P.Exh. 85].

283. IP filtering can lead to blocking because of the prevalence of "shared IP addresses," as detailed above. If an ISP uses IP filtering to block access to a particular IP address, *all* web sites hosted at that IP address are blocked. Thus, in the hypothetical example of an Informal Notice directing an ISP to block access to Professor Marcus's web site www.cis.upenn.edu, an ISP's use of IP filtering to block access to 158.130.12.9 would also block access to a second web site, hlt2002.org. [Tr. 1/6/04 pp.103-04 (M.Marcus)]. As a more concrete example, in response to Informal Notice 2545 (which directed Epix.net to block access to www.RedactedURL4.com) 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. [P.Exh. 54 (Informal Notice 2545); P.Exh. 56 (internal Epix.net e-mail indicating that 204.251.10.203 blocked in order to block access to www.RedactedURL4.com); Section IX.B below].

284. As detailed in the specific subsections, at least one million of the blocked web sites detailed in Section IX.C were (and in many cases are) blocked as a direct result of the use of IP filtering.

285. The technical method disfavored by the ISPs – the DNS filtering method – also creates a high risk of blocking innocent content. For example, the DNS filtering method will block multiple web sites unrelated to the target of the blocking order if those web sites are hosted as "sub-pages" of a given domain name. This situation can happen with "online communities" such as the GeoCities web site, which allows many different users to have web sites on subpages of GeoCities.com, such as http://www.geocities.com/example/index.html. In this case, as both Professor Marcus and Ben Stern agreed, if any of the web sites are blocked using the DNS filtering method, all of the web sites that operate as subpages under the same domain will be blocked. [Tr. 1/6/04 pp.109-10 (M.Marcus); Tr. 2/18/04 pp.54-56, 60 (B.Stern)]. All subpages

of a single domain would also be blocked by IP filtering. [*See* Section II.F (entire domain falls

under the same IP address)].

286. In another example, if a blocking order were entered against any of the independent

web sites hosted by the www.webspawner.com web hosting company (*see* ¶ 93 above) and an

ISP used DNS filtering, then all of the web sites hosted under that domain name would be

blocked, including the web sites of the Pennsylvania Performing Arts Academy

(http://www.webspawner.com/users/paperformingarts/index.html), a Steelton, Pennsylvania

Masonic Lodge (http://www.webspawner.com/users/paxton/index.html), and a London, England,

rugby football team (http://www.webspawner.com/users/londonbroncos16/index.html). [Tr.

1/6/04 pp.110-14 (M.Marcus); P.Exh. 104, Tab 6].

287. As will be discussed further below, Verizon blocked the online community

"Terra.es" when it instituted a DNS filter in response to an Informal Notice. Verizon engineer

Richard Hiester, who received the request to remove the block on the Terra.es domain, was not

surprised; he said "it was the request we were expecting to see some day where we were being

asked to block something that large that would have a large impact." [Dep. of R.Hiester

(Verizon) at 61].

288. Defendant's expert witness Ben Stern admitted that DNS filtering could lead to the

blocking of innocent web sites, and he specifically admitted a regime of DNS filtering would

cause the blockage of hundreds of thousands of Terra.es web sites as detailed in Section IX.C.2

below, and hundreds of thousands of Digilander.libero.it web sites as detailed in Section IX.C.7

below. [Tr. 1/29/04 pp.50-51 (B.Stern); Tr. 2/18/04 pp.52-53 (B.Stern)]

B. The Blockage of Laura Blain's Web Sites

289. The hardship faced by Bradford County, Pennsylvania, webmaster Laura Blain as a result of an Informal Notice issued to her ISP demonstrates the problems created by the OAG's enforcement scheme. In July 2003, as a result of Informal Notice 2545, the Pennsylvania-based ISP Epix.net blocked access to a web server of a major web hosting company directNIC, at the IP address 204.251.10.203, thereby blocking access to, among other sites, the web sites of a non-profit community recreation center and a community school, both located in Bradford County, Pennsylvania. [*See* paragraphs immediately following].

290. Witness Laura Blain served as the webmaster for a number of community organizations in rural Pennsylvania, including the Sheshequin-Ulster Community Center. Ms. Blain created the web site for the community center in February 2003 in part to address an important need to share information with township officials who controlled funding for the center. [Tr. 1/6/04 pp.26,28 (L.Blain)]. 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 27-28; P.Exh. 104 Tab 8 (screen shots from http://www.sheshequinulsterreccenter.org/)].

291. Ms. Blain set up the community center's web site using the directNIC web hosting company, in part because of its relatively low cost. [Tr. 1/6/04 p.26 (L.Blain)]. In exchange for the placement of two small "banner" advertisements on the community center's web site, the directNIC company hosts the web site for free. [*Id.* at 27-28].

292. Laura Blain also created a web site for the "Pennsylvania Hinterland Cyber Charter School" based in Ulster, Pennsylvania. [Tr. 1/6/04 pp.28-30 (L.Blain); P.Exh. 55 (screen shot from http://pahinterlandschool.org)]. Again she chose to use the directNIC web hosting service,

but opted to get an advertisement-free web site by paying a fee to directNIC to host the web site. [Tr. 1/6/04 p.29 (L.Blain)].

293.   To gain access to the Internet, Ms. Blain used the services of a local Pennsylvania ISP, Epix.net, which provides both high-speed DSL service at her home and dial-up service at her office. [Tr. 1/6/04 p.24 (L.Blain)]. This service relationship is wholly unrelated to the web hosting relationships that Ms. Blain maintained with the directNIC web hosting company.

294.   On July 1, 2003, the OAG issued Informal Notice 2545 to the Epix.net ISP based in Dallas, Pennsylvania, directing Epix.net to block access to www.RedactedURL4.com. [P.Exh. 54 (Informal Notice 2545); Jt.Exh. 9, Tab A, line 324 (listing Notice 2545)]. As a result of that Informal Notice, Epix.net blocked access to IP address 204.251.10.203. [P.Exh. 56 (internal Epix.net e-mail indicating that 204.251.10.203 blocked in order to block access to www.RedactedURL4.com)].

295.   IP address 204.251.10.203 was the IP address that directNIC had assigned to both the community center and the school web sites that Ms. Blain operated. [P.Exh. 53, pp.5, 6 (showing results of "ping" and "tracert" tests for Ms. Blain's web sites)].

296.   In early July 2003, it came to Laura Blain's attention that the community center web site was – for a then unexplained reason – 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. 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 attempt to determine why the web sites were not available. After extensive testing by directNIC and by Ms. Blain over the course of five days, directNIC determined that the problem was not with the web hosting company, but with the ISP who was providing Ms. Blain's Internet access –

Epix.net. [Tr. 1/6/04 pp.30-31, 42 (L.Blain); P.Exh. 53 (screenshot of communications between Blain and directNIC)].

297. Ms. Blain next contacted her ISP, Epix.net, to ask why she could not access her sites. Ms. Blain was told by Epix.net that it would investigate, but in the meantime she was still unable to access her sites, and thus she had to return to directNIC to ask that the web hosting company move the web sites to a different IP address, a process that took a couple of days. [Tr. 1/6/04 pp.37-38, 40-41 (L.Blain); P.Exh. 53 (screenshot of communications between Blain and directNIC)].

298. 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. Thus, the unavailability could have been seriously damaging to the center. [Tr. 1/6/04 pp.37-38 (L.Blain)].

299. For Ms. Blain's other web site that was blocked by Epix.net – the charter school's site – Ms. Blain concluded that the school could not afford to be "off-line" for the time it would take for directNIC to move the web site to a new IP address, and thus Ms. Blain was forced to purchase web hosting services from another company entirely. [Tr. 1/6/04 p.38 (L.Blain)].

300. According to Epix.net employees, after hearing from Ms. Blain the technical support department at Epix.net determined that the sites were hosted on an IP address that had been blocked in response to an Informal Notice, and notified Gary Basham, the systems engineering manager. [Dep. of G.Basham (Epix) at 54-57].

301. On July 9, 2003, Mr. Basham notified Susan Butchko-Krisa, in the legal department at Epix.net, that a customer was unable to access a site that shared an IP address with a site that

had been identified in an Informal Notice, which IP address had been blocked by Epix.net. [P.Exh. 56]

302. Mr. Basham and Ms. Butchko-Krisa then participated in a call with Special Agent Guzy Sr. of the Office of the Attorney General. The Epix.net representatives explained the problem with the blocked site, and the two methods of compliance they were using at that time, IP filtering and DNS filtering. Special Agent Guzy Sr. told them that he would have Chief Deputy Burfete call them. [Dep. of S.Butchko-Krisa (Epix) at 10-13, 28; Dep. of G.Basham (Epix) at 20-22, 57-65].

303. Chief Deputy Burfete called Ms. Butchko-Krisa on July 10, 2003, and she explained that innocent web sites had been blocked as a result of the Informal Notice. He told her that he was aware that IP filtering could result in the blocking of additional sites. He also stated that Epix.net was not required to institute IP filtering and could rely on DNS filtering alone. [Tr. 1/8/04 pp.68-70 (J.Burfete); P.Exh. 54 (notes of conversation between J.Burfete & Epix); P.Exh. 57; Dep. of S.Butchko-Krisa (Epix) at 19-21.]

304. After that conversation, Epix.net changed its policy to relying solely on DNS filtering, 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]. Ms. Butchko-Krisa claimed in her deposition that Epix.net lifted the IP address block of Ms. Blain's sites after she spoke to Special Agent Guzy, but Ms. Blain remained unable to access the sites through Epix.net until they were moved to new IP addresses. [Tr. 1/6/04 pp. 37-38, 40-41 (L.Blain); P.Exh. 53; Dep. of S.Butchko-Krisa (Epix) at 28].

305. Beyond Ms. Blain's web sites – http://www.sheshequinulsterreccenter.org/ and http://pahinterlandschool.org – the record does not reflect how many *other* web sites Epix.net

blocked access to in July 2003 when it blocked access to IP address 204.251.10.203. At Ms.

Blain's request, however, her web hosting company, directNIC, moved her community center

web site to another of its web servers (with a different IP address). [*See* paragraphs above]. As

of October 2003, when Plaintiffs' expert Clark conducted his research into IP address sharing,

Ms. Blain's web site shared its new IP address (204.251.10.203) with at least 15,574 other

domains. [Tr. 1/7/04 pp.141-42 (M.Clark)]. Given that Ms. Blain did not change or upgrade her

service when she asked directNIC to move her http://www.sheshequinulsterreccenter.org/

domain to a new IP address, it appears likely that in July 2003 Epix.net blocked access to

thousands of other web sites in addition to Ms. Blain's (and Ms. Blain was the first to notice to

blockage).

C. Instances of Innocent Blocked Web Sites

306. Laura Blain is just one example of the results of the Statute and Informal Notices.

From early on and continuing through today, the ISPs' compliance with the Informal Notices

directly led to the blocking of many more innocent web sites. In total, more than 1.5 million

lawful web sites were blocked as a result of Informal Notices (and well over half a million

remain blocked today). [*See* paragraphs immediately following].

1. June 2002 – 500,000 or More Web Sites Hosted by the MyDomain.com Web Hosting Company, Blocked by the AOL ISP

307. In June 2002 – within the first six weeks of the OAG's Informal Notice process – as

a result of Informal Notice 7003, the ISP AOL blocked access to a web server of the

MyDomain.com web hosting company, thereby blocking access to at least 500,000 web sites.

[*See* paragraphs immediately following].

308. On June 3, 2002, the OAG issued Informal Notice 7003 to the AOL ISP, directing AOL to block access to www.RedactedURL5.com. [P.Exh. 47 (Informal Notice 7003); Jt.Exh. 9, Tab C, line 17 (listing Notice 7003)]. As a result of that Informal Notice, AOL blocked access to IP address 216.148.221.150. [P.Exh. 46 (internal AOL spreadsheet indicating that 216.148.221.150 was blocked in order to block access to www.RedactedURL5.com)].

309. Soon thereafter, the web hosting company that hosted that IP address, MyDomain.com, noticed a dramatic drop in traffic to hundreds of thousand of web sites. It took the hosting company days to investigate, and ultimately determine that it was no longer getting any traffic from AOL. The general counsel of MyDomain.com contacted Christopher Bubb of AOL late on a Friday afternoon, who determined that the block had been instituted in response to an Informal Notice from the OAG. He asked the web hosting company to take down the offending site, it did, and AOL released the IP address block within a few hours. [Dep. of C.Bubb (AOL) at 54-62, 70].

310. The following Monday, AOL alerted the OAG of the fact that a single Informal Notice had led to the blocking of a massive number of unrelated web sites and the steps it had taken to address the problem, and indicated frustration that no one from the OAG had been available on Friday to deal with what AOL considered an important and time-sensitive matter. In further conversations with the web hosting company, the OAG legal adviser learned that half a million web sites were sharing the IP address that AOL had blocked. [Tr. 1/8/04 pp.63-65 (J.Burfete); P.Exh. 48; Dep. of C.Bubb (AOL) at 61-62].

2. August 2002 – Hundreds of Thousands of Web Sites Hosted by the Terra.es Web Hosting Company, Blocked by the Verizon ISP

311. In August 2002, as a result of Informal Notice 5924, the ISP Verizon blocked access to a web server of the Terra.es web hosting company, thereby blocking access to as many as 500,000 web sites. [*See* paragraphs immediately following].

312. On August 13, 2002, the OAG issued Informal Notice No. 5924, directing Verizon to block access to http://www.terra.es/personal9/cppornosite/. [Jt.Exh. 9, Tab B, line 407 (listing Notice 5924)]. As a result of that Informal Notice, Verizon blocked access to the entire Terra.es domain, and sent a confirmation of that block to the OAG on August 16, 2002. [Dep. of S.Lebredo (Verizon) at 51-52, 55-58; P.Exh. 84].[13]

313. As OAG legal adviser John Burfete understood, 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." [P.Exh. 32].

314. Two or three weeks later, Verizon was contacted by Lycos, a U.S. company that owned Spain-based Terra.es, and informed that Verizon customers could not access Terra.es sites. Concerned that Terra.es was "a sizable business that our customers wanted to utilize," Verizon asked Terra.es and Lycos to have the offending content removed, so that Verizon could then remove its block of the Terra.es domain. [Dep. of S.Lebredo (Verizon) at 51-52, 57-49]. Verizon then removed the block on the domain. [Dep. of R.Hiester (Verizon) at 61].

315. Following is a sample of the constitutionally protected content on Terra.es blocked as a result of Informal Notice 5924:

---

[13] As noted in text, Verizon's Scott Lebredo testified in deposition that Verizon's blocking of Terra.es first arose in mid-August 2002, and was resolved two to three weeks later. [Dep. of S.Lebredo (Verizon) at 51-58]. In fact, Verizon first received blocking orders concerning Terra.es at the very end of July 2002, and thus it is likely that Verizon's blocking of Terra.es started in *early* August and lasted four to five weeks. [Jt.Exh. 9, Tab A, lines 397-406].

- Web site of the Bioterrorism Safety Council, at
  http://www.terra.es/personal5/safetycouncil/

- Web site of the ITGE Geological Survey of Spain, at
  http://www.terra.es/personal/lsomoza/marina/proyectos.html

- Web site of the International Philatelic Club, at
  http://www.terra.es/personal/jla31291/home.htm

[Tr. 1/28/04 pp. 25-26 (M.Clark); P.Exh. 104, Tab 9]. The Attorney General has acknowledged

that these sites do not contain child pornography. [P.Exh. 74, ¶ 1].

316. Plaintiffs' expert Michael Clark used a well-known Internet tool called the

"Wayback Machine" to determine that those same three web sites listed in the paragraph above

also were in existence prior to August 16, 2002, when Terra.es was blocked by Verizon. [Tr.

1/28/04 pp. 26-27 (M.Clark); P.Exh. 104, Tab 10].

3. September 2002 – Tens of Thousands of Web Sites Hosted by the About.com Web Hosting Company, Blocked by the AOL ISP

317. In September 2002, as a result of Informal Notice 3627, the ISP AOL blocked

access to a web server of the About.com web hosting company, thereby blocking access to

reportedly five million web sites. [*See* paragraphs immediately following].

318. On September 6, 2002, the OAG issued Informal Notice 3627 to the AOL ISP,

directing AOL to block access to www.preteens.freeservers.com. [Jt.Exh. 9, Tab D, line 313

(listing Notice 3727)]. As a result of that Informal Notice, AOL blocked access to IP address

208.185.127.162. [P.Exh. 46, 3rd page (internal AOL spreadsheet indicating that

208.185.127.162 has blocked in order to block access to www.preteens.freeservers.com)].

319. AOL testified in deposition that it blocked tens of thousands of web sites hosted by

a company named About.com in September 2002. [Dep. of C.Bubb (AOL) at 147-48].

320. AOL alerted the OAG of the fact that Informal Notice 3627 had led to the blocking

of a massive number of web sites hosted by the About.com web hosting company. According to

contemporaneous notes made by OAG legal adviser John Burfete, AOL reported that as many as

five million web sites hosted by About.com were blocked. [Tr. 1/9/04 p.28 (J.Burfete); P.Exh.

82, 3rd page[14]].

4.   September 2002 – 559 or More Web Sites Hosted by the Tuportal.com Web Hosting Company, Blocked by the AOL ISP

321. In September 2002, as a result of Informal Notice 1086, the ISP AOL blocked

access to a web server of the Tuportal.com web hosting company, thereby blocking access to at

least 559 web sites, at least 546 of which remain blocked as of the trial in this case. [*See*

paragraphs immediately following].

322. On September 6, 2002, the OAG issued Informal Notice 1086 to the AOL ISP,

directing AOL to block access to http://www.girlsroom.tuportal.com/two.html. [P.Exh. 96A

(Informal Notice); Jt.Exh. 9, Tab B, line 212 (listing Notice 1086)]. As a result of that Informal

Notice, AOL on September 13, 2002, blocked access to IP address 217.116.4.196. [P.Exh. 46,

3rd page (internal AOL spreadsheet indicating that 217.116.4.196 was blocked in order to block

access to http://www.girlsroom.tuportal.com/two.html)].

323. Plaintiffs' expert Michael Clark researched the IP address 217.116.4.196 to

determine what other web sites shared that IP address. By utilizing the database of shared IP

---

[14] Based on the pages in P.Exh. 82, it appears either that certain pages were misfiled by the OAG, or the OAG
used the same Informal Notice number for two different ISPs sent on more than two months apart (something
that is possible given the confusion in Informal Notice numbering). The third page of P.Exh. 82 refers to
blockages of web sites hosted by About.com as a result of Informal Notice 3627 sent to AOL, which Jt.Exh. 9
confirms was sent to AOL on Sept. 6, 2002, concerning the URL http://www.preteen.freeserver.com. If
needed, the Court can take judicial notice of the fact that About.com owns freeserver.com. *See*
http://siliconalley.venturereporter.net/issues/sar03012000.html.   Other pages of P.Exh. 82 apparently refer to a
different Informal Notice numbered 3627, although it is likely that those references are incorrect.

addresses that he had created in the fall of 2003 (and other Internet search methods), and by verifying that the sites he found still had that IP address, Mr. Clark was able to determine that at least 546 web sites shared the IP address 217.116.4.196 as of January 24, 2004. [P.Exh. 96B; Tr. 1/27/04 pp. 180-82 (M.Clark)].

324. Christopher Bubb of AOL confirmed that as of October 3, 2003, AOL's IP address blocks remained in place. [Dep. of C.Bubb (AOL) at 140].

325. The 546 web sites listed in P.Exh. 96B represent some, but not all, of the web sites that are blocked today as a result of Informal Notice No. 1086 issued to AOL. Plaintiffs have identified at least one other site – club.imagenysonido.com – that shares the IP address 217.116.4.196 and has therefore been blocked as a result of Informal Notice 1086 but is not listed on P.Exh. 96B. [Tr. 1/28/04 pp. 187-88 (M.Clark)]. Because of the inherent limitations in Plaintiffs' ability to identified blocked sites, *see, e.g.,* Jt.Stip. 59, Plaintiffs believe that there exist a significant number of additional web sites blocked by this Informal Notice that Plaintiffs have yet to identify.

326. P.Exh. 5 provides a sample of the constitutionally protected content blocked as a result of Informal Notice 1086, including:

- http://isladeesculturas.tuportal.com/page2.html (a guide to the Spanish "Island of Sculptures" of Pontevedra)

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

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

[P.Exh. 5; P.Exh. 96B; ; P.Exh. 104, Tab 11; Tr. 1/7/04 pp.183-99 (M.Clark)]. The Attorney General has acknowledged that these sites do not contain child pornography. [P.Exh. 74, ¶ 1].

327. One of these web sites, for example, is the home page of the "Island of Sculptures" in Pontevedra, Spain, which appears to be a significant cultural site in Spain. [facts susceptible to judicial notice, specifically the results of a search on Google.com for "island of sculptures" (in quotes), http://www.google.com/search?q=%22island+of+sculptures%22]. [P.Exh. 104, Tab 11]

328. For each of the three web sites listed above, Mr. Clark testified how he was able to access the web sites through the services of the ISP WorldCom, but he was unable to access the web sites when he attempted to access them through the ISP AOL (which was the recipient of Informal Notice 1086). Instead of gaining access to the web sites, the web browser displayed the following message:

> **Web Site Not Responding**
>
> The web site you have requested may be experiencing technical difficulties due to a busy or broken server.
>
> Please try again by clicking the **Reload** icon on your navigation bar or, if that does not work, you may want to return to the site at a later time.

[Tr. 1/7/04 pp.183-90 (M.Clark); P.Exh. 5; Tr. 1/27/04 pp. 182-83 (M.Clark)].

329. Mr. Clark also determined that the IP address 217.116.4.196 and therefore the web sites listed on P.Exh. 96B remained blocked by AOL as of the trial. He demonstrated in court that he was able to access two web sites listed on P.Exh. 96B (isladeesculturas.tuportal.com and dragon.tuportal.com) through the WorldCom ISP, but he was not able to access those same sites through the AOL ISP. [Tr. 1/28/04 pp. 163-69, 180, 182; P.Exhs. 109, 110, 111, 116].

5. November 2002 – 124 or More Web Sites at the IP Address 207.44.156.52, Blocked by the AOL ISP

330. In November 2002, as a result of Informal Notice 2966, the ISP AOL blocked access to a web server at the IP address 207.44.156.52, thereby blocking access to at least 124

web sites, at least 120 of which remain blocked as of the trial in this case. [*See* paragraphs immediately following].

331. On November 4, 2002, the OAG issued Informal Notice 2966 to the AOL ISP, directing AOL to block access to http://www.baby-sex.com/index.php. [P.Exh. 97A (Informal Notice); Jt.Exh. 9, Tab B, line 154 (listing Notice 2966)]. As a result of that Informal Notice, AOL on November 22, 2002, blocked access to IP address 207.44.156.52. [P.Exh. 46, 4th page (internal AOL spreadsheet indicating that 207.44.156.52 was blocked in order to block access to http://www.baby-sex.com/index.php)].

332. Plaintiffs' expert Michael Clark researched the IP address 207.44.156.52 to determine what other web sites shared that IP address. By utilizing the database of shared IP addresses that he had created in the fall of 2003, and by verifying that the sites he found still had that IP address, Mr. Clark was able to determine that at least 120 web sites shared the IP address 207.44.156.52 as of January 24, 2004. [P.Exh. 97B; Tr. 1/27/04 pp. 185-87 (M.Clark)].

333. Christopher Bubb of AOL confirmed that as of October 3, 2003, AOL's IP address blocks remained in place. [Dep. of C.Bubb (AOL) at 140].

334. P.Exh. 5 provides a sample of the constitutionally protected content blocked as a result of Informal Notice 2966, including:

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

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

[P.Exh. 5; P.Exh. 97B; P.Exh. 104, Tab 11; Tr. 1/7/04 pp.183-90 (M.Clark)]. The Attorney General has acknowledged that these sites do not contain child pornography. [P.Exh. 74, ¶ 1].

335. For each of the two web sites listed above, Mr. Clark testified how he was able to access the web sites through the services of the ISP WorldCom, but he was unable to access the

web sites when he attempted to access them through the ISP AOL (which was the recipient of

Informal Notice 1086). Instead of gaining access to the web sites, the web browser displayed the

following message:

> **Web Site Not Responding**
>
> The web site you have requested may be experiencing technical
> difficulties due to a busy or broken server.
>
> Please try again by clicking the **Reload** icon on your navigation
> bar or, if that does not work, you may want to return to the site at a
> later time.

[Tr. 1/7/04 pp.183-90 (M.Clark); P.Exh. 5; Tr. 1/27/04 pp. 187 (M.Clark)].

336. Mr. Clark also determined that the IP address 207.44.156.52 and therefore the web

sites listed on P.Exh. 97B remained blocked by AOL as of the trial. He demonstrated in court

that he was able to access two web sites listed on P.Exh. 96B (www.vermontgiftbasket.us and

www.movieposterforsale.us) through the WorldCom ISP, but he was not able to access those

same sites through the AOL ISP. [Tr. 1/28/04 pp. 169-70, 176-77, 179-82; P.Exhs. 112, 113,

114, 115].

6. February 2003 – 3,988 or More Web Sites Hosted by the Digipocket.com (.hk.st) Web Hosting Company, Blocked by the Comcast ISP

337. In February 2003, as a result of Informal Notice 1519 (targeted at the URL

http://juventa.hk.st), the ISP Comcast blocked access to a web server of the Digipocket.com web

hosting company, at the IP addresses 202.181.231.211 and 202.181.231.212, thereby blocking

access to at least 3,988 web sites, at least 3,962 of which remain blocked as of the trial in this

case. [*See* paragraphs immediately following].

338. On February 4, 2003, the OAG issued Informal Notice 1519 to the Comcast ISP,

directing Comcast to block access to http://juventa.hk.st. [P.Exh. 98A (Informal Notice); Jt.Exh.

9, Tab B, lines 49-50 (listing Notice 1519)]. As a result of that Informal Notice, Comcast blocked access to IP addresses 202.181.231.211 and 202.181.231.212. [Jt.Exh. 9, Tab B, lines 49-50].

339. Plaintiffs' expert Michael Clark researched the IP addresses 202.181.231.211 and 202.181.231.212 to determine what other web sites shared that IP address. By utilizing the database of shared IP addresses that he had created in the fall of 2003 and other Internet search methods, Mr. Clark was able to determine that at least 3,988 web sites shared the IP addresses 202.181.231.211 and 202.181.231.212 as of November 2003. When he verified those sites again in early January 2004, he determined that 3,962 sites still shared those IP addresses. [P.Exh. 80C; Tr. 1/27/04 pp. 192-95, 199-200 (M.Clark); Tr. 1/28/04 pp. 96-97 (M.Clark)].

340. Comcast confirmed in its deposition that all of the IP address blocks that it instituted in response to an Informal Notice remained in place as of October 23, 2003. [Dep. of G.Lipscomb (Comcast) at 107].

341. Although Michael Clark's research only verified that certain web sites that existed in October and November of 2003 remain blocked, OAG technical staff member Dennis Guzy Jr. confirmed that additional hk.st domain names created more recently are also blocked by Comcast. According to his testimony, soon before trial Mr. Guzy created a *new* .hk.st web site, and immediately was able to confirm that the newly created web site was blocked.   [Tr. 1/12/04 pp.47-48 (D.GuzyJr.)]. Thus, in addition to the web sites that Plaintiffs have established are blocked by Comcast, any recently created .hk.st web sites are also blocked.

342. P.Exh. 95 provides a sample of the constitutionally protected content blocked as a result of Informal Notice 1519, including:

- http://crystalplus.hk.st (jewelry maker)

- http://seasons-home.hk.st (web site about Seasons Lee, a Hong Kong rock musician)[15]

- http://illuminati.hk.st (an authors' self-publication site)

- http://photonet.nk.st (web site of the Photo On Net Photography Society)

- http://www.digipocket.com (the hk.st web hosting company)

[P.Exh. 95]

343. For each of the five web sites listed above, Alexander Roszko explained in his

Verification (P.Exh. 95) how he was able to access the web sites through the services of the ISP

DCAnet, but he was unable to access the web sites when he attempted to access them through the

ISP Comcast (which was the recipient of Informal Notice 1519). Instead of gaining access to the

web sites, the web browser displayed (for four of the five sites) the following message:

> **This page cannot be displayed**
>
> The page you are looking for is currently unavailable. The Web
> site might be experiencing technical difficulties, or you may need
> to adjust your browser settings.

[P.Exh. 95]. Based on Mr. Roszko's verification, Mr. Clark concluded that Comcast instituted a

block on the IP address of the sites listed in P.Exh. 80C, and that those sites would not be

accessible through Comcast. [Tr. 1/28/04 pp. 184-85 (M.Clark)].

344. Displayed on the home page of the www.hk.st web hosting company is a statement

that reads "Please report illegal content or abuse to abuse@hk.st." [Tr. 1/12/04 pp.175-76

(D.GuzyJr.); D.Exh. 15]. Had the OAG contacted the web hosting company and thereby had

them remove the http://juventa.hk.st web site, there would be three results:

---

[15] To the extent the Court needs to review web sites in the Chinese language, those web sites can be roughly translated using the services found at http://babelfish.altavista.com.

- the child pornography content would have been removed from the entire Internet (instead of just Comcast subscribers),

- there would have been no need to send any blocking order to Comcast, and

- Comcast would not have blocked access to thousands of web sites.

345. Indeed, it appears that sometime after the OAG sent the informal notice to Comcast, someone *did* contact the web hosting company to report the illegal content on http://juventa.hk.st. If one accesses that web site today, the following message is displayed: "This account has been terminated due to the violation of FREE SiTE Domain service regulations." [facts susceptible to judicial notice].

346. Based on the Court's experience with electronic mail, the Court can take judicial notice of the fact that it would have taken the OAG no more than 5 to 10 minutes to transmit an e-mail to abuse@hk.st alerting the web hosting company to the child pornography located at http://juventa.hk.st. Based on the facts in this subsection, had in February 2003 the OAG sent such an e-mail, then thousands of lawful web sites would not have been blocked since February 2003 (and continuing to the present).

347. Even if one were to hypothesize that the Informal Notice system is constitutional, the fact that the http://juventa.hk.st web site no longer contains child pornography [*see* ¶ 345 above] indicates that the continuing blocking by Comcast of thousands of web sites as a result of Informal Notice 1519 serves no governmental purpose whatsoever.

7. March 2003 – 342,080 or More Web Sites Hosted by the Digilander.it Web Hosting Company, Blocked by the Comcast ISP

348. In March 2003, as a result of Informal Notices 1933 and 1947, the ISP Comcast blocked access to a web server of the Digilander.it web hosting company, at the IP address 195.210.93.172, thereby blocking access to at least 342,080 web sites, and blocking access to at

96

least 491,850 total sites by the time of the trial in this case. [*See* paragraphs immediately following].

349. On March 25, 2003, the OAG issued Informal Notices 1933 and 1947 to the Comcast ISP, directing Comcast to block access to http://digilander.libero.it/RedactedURL30 and http://digilander.libero.it/RedactedURL31. [P.Exh. 99A (Informal Notice No. 1933); Jt.Exh. 9, Tab B, lines 34-35 (listing Notices 1933 and 1947)]. As a result of those Informal Notices, Comcast on April 1, 2003, blocked access to IP address 195.210.93.172. [P.Exhs. 44, 99A; Jt.Exh. 9, Tab B, lines 34-35].

350. Plaintiffs' expert Michael Clark researched the IP address 195.210.93.172 and determined that an Italy-based web hosting service, Digilander, uses that IP address for its digilander.libero.it domain. The Digilander site contains an index of the web sites that it hosts, which Mr. Clark used to compile a list of the various web sites that were hosted under the digilander.libero.it domain name and that therefore shared that IP address. Mr. Clark was able to determine that at least 342,080 web sites shared the IP address 195.210.93.172 as of November 2003. When he reviewed the index of sites listed on the Digilander site again in early January 2004, he determined that it listed 491,850 web sites. It appeared that maintenance had been done on the Digilander site in the interim, which Mr. Clark believed explained the discrepancy. [P.Exhs. 80D1, 80D2, 80D3; Tr. 1/27/04 pp. 203-05 (M.Clark); Tr. 1/28/04 pp. 3-6 (M.Clark)].

351. Comcast confirmed in its deposition that all of the IP address blocks that it instituted in response to an Informal Notice remained in place as of October 23, 2003. [Dep. of G.Lipscomb (Comcast) at 107].

352. P.Exh. 95 provides a sample of the constitutionally protected content blocked as a result of Informal Notices 1933 and 1947, including:

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

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

See also screenshots of http://digilander.libero.it/rab002/, http://digilander.libero.it/webphoto/, http://digilander.libero.it/igniferal/home/. [P.Exh. 95; P.Exh. 104, Tab 12]. The Attorney General has acknowledged that these sites do not contain child pornography. [P.Exh. 74, ¶ 1].

353. For each of the five web sites listed above, Alexander Roszko explained in his Verification (P.Exh. 95) how he was able to access the web sites through the services of the ISP DCAnet, but he was unable to access the web sites when he attempted to access them through the ISP Comcast (which was the recipient of Informal Notices 1933 and 1947). Instead of gaining access to the web sites, the web browser displayed the following message:

> **This page cannot be displayed**
>
> The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.

[P.Exh. 95].

8. Approximately February or March 2003 – At Least Two Unidentified Incidents of Blocking of Innocent Content by the Comcast ISP

354. When Comcast first started receiving Informal Notices, it blocked an entire hosting company. It received complaints both from people who called and indicated they could not access the sites, and from the hosting company itself. When Comcast employee Gary Lipscomb explained to the hosting company the nature of the problem, it agreed to take down the offending material, and Comcast removed the block. [Dep. of G.Lipscomb (Comcast) at 49-50, 65-67].

355. Comcast also had a second instance of blocking sites that were not specified in an Informal Notice, although Comcast employee Gary Lipscomb did not recall the details of that instance. In response to a complaint in that situation, Comcast reversed the block it had instituted. [Dep. of G.Lipscomb (Comcast) at 65-67].

9. June 2003 – 331,066 or More Web Sites Hosted by the .da.ru Web Hosting Company, Blocked by the Comcast ISP

356. In June 2003, as a result of Informal Notice 2383 (targeting the URL http://wildorchiday.da.ru), the ISP Comcast blocked access to a web server of the da.ru web hosting company, at the IP address 213.59.0.84, thereby blocking access to at least 331,066 web sites, at least 326,050 of which remain blocked as of the trial in this case. [*See* paragraphs immediately following].

357. On June 11, 2003, the OAG issued Informal Notice 2383 to the Comcast ISP, directing Comcast to block access to http://wildorchiday.da.ru. [P.Exh. 100A (Informal Notice); Jt.Exh. 9, Tab B, line 110 (listing Notice 2383)]. As a result of that Informal Notice, Comcast on June 18, 2003, blocked access to IP address 213.59.0.84. [P.Exh. 100A; Jt.Exh. 9, Tab B, line 110].

358. Plaintiffs' expert Michael Clark researched the IP address 213.59.0.84 and found no sites with that IP address in the database he had created in November 2003 because that database did not contain foreign web sites. He then went to www.da.ru, the parent domain of the site subject to Informal Notice 2383, and found a list of web sites hosted on that domain, which is based in Russia. Using that list, Mr. Clark was able to determine that the www.da.ru domain contained at least 331,066 web sites as of November 2003, as shown in P.Exh. 80E. When he reviewed the list of sites at www.da.ru again in early January 2004, he determined that it contained 334,395 web sites. In mid-February 2004, he verified whether the sites listed on

P.Exh. 80E resolved to the IP address 213.59.0.84 and found that 326,050 web sites resolve to that IP address. [P.Exhs. 80E1, 80E2; Tr. 1/28/04 pp. 8-11 (M.Clark); Tr. 2/26/04 pp. 58-60 (M.Clark)].

359. Mr. Clark also evaluated how many of those 326,050 web sites are active sites. He researched every thousandth domain, and found that ten domains had no content, 45 domains returned the home page of the parent domain, www.da.ru [D.Exh. 16], and 271 were active sites with their own content. Thus, he concluded that approximately 271,000 domains are both at the IP address 213.59.0.84 and are active sites with their own content. [Tr. 2/26/04 pp. 60-62, 66-67 (M.Clark)].

360. Comcast confirmed in its deposition that all of the IP address blocks that it instituted in response to an Informal Notice remained in place as of October 23, 2003. [Dep. of G.Lipscomb (Comcast) at 107].

361. Although the above evidence only assessed the availability of certain web sites that existed in November 2003, OAG technical staff member Dennis Guzy Jr. confirmed that additional .da.ru domain names created more recently are also blocked by Comcast. [Tr. 1/12/04 pp.50-52 (D.GuzyJr.)].

362. P.Exh. 95 provides a sample of the constitutionally protected content blocked as a result of Informal Notices 2383, including:

- http://ecomics.da.ru (Russian language comics and comic artwork, including English translations)

- http://engtimeline.da.ru (a history of the English language)

- http://0987654321.da.ru (a student's school pictures)

[P.Exh. 95]

363. For each of the three web sites listed above, Alexander Roszko explained in his

Verification (P.Exh. 95) how he was able to access the web sites through the services of the ISP

DCAnet, but he was unable to access the web sites when he attempted to access them through the

ISP Comcast (which was the recipient of Informal Notice 2383). Instead of gaining access to the

web sites, the web browser displayed the following message:

> **This page cannot be displayed**
>
> The page you are looking for is currently unavailable. The Web
> site might be experiencing technical difficulties, or you may need
> to adjust your browser settings.

[P.Exh. 95].

364. For each of those three sites, in February 2004 Mr. Clark verified that they resolved

to the IP address that had been blocked, 213.59.0.84, that he was able to access them over the

WorldCom ISP, which was not subject to a blocking order with respect to www.da.ru, and that

they contained active content. [Tr. 2/26/04 pp. 63-64, 67 (M.Clark)].

365. In addition, other constitutionally protected content blocked as a result of Informal

Notices 2383 include:

- http://chrisenglish.da.ru (a London classical guitarist) [P.Exh. 86]

- http://ieclub.da.ru (a Russian English language club) [P.Exh. 87]

- http://dalmation.da.ru (an Ohio family's web site) [P.Exh. 88]

366. Displayed on the home page of the www.da.ru web hosting company is a statement

that reads "Spammers, warez, child porn, pirated MP3s, Nazi sites, and any kind of illegal

activity are prohibited. Send complaints to policy@da.ru if found." [Tr. 1/12/04 p.176

(D.GuzyJr.); D.Exh. 16]. Had the OAG contacted the www.da.ru web hosting company and

thereby had them remove the http://wildorchiday.da.ru web site, there would be three results:

- the child pornography content would have been removed from the entire Internet (instead of just Comcast subscribers),

- there would have been no need to send any blocking order to Comcast, and

- Comcast would not have blocked access to hundreds of thousands of web sites.

367. Indeed, it appears that sometime after the OAG sent the informal notice to Comcast, someone *did* contact the web hosting company to report the illegal content on http://wildorchiday.da.ru. If one accesses that web site today, the following message is displayed: "The site you are looking for is closed due to non-ethical and/or abusive activity." [Tr. 1/12/04 pp.176-77 (D.GuzyJr.); P.Exh. 94].

368. Based on the Court's experience with electronic mail, the Court can take judicial notice of the fact that it would have taken the OAG no more than 5 to 10 minutes to transmit an e-mail to policy@da.ru alerting the web hosting company to the child pornography located at http://wildorchiday.da.ru. Based on the facts in this subsection, had in June 2003 the OAG sent such an e-mail, then hundreds of thousands of lawful web sites would not have been blocked since June 2003 (and continuing to the present).

369. Even if one were to hypothesize that the Informal Notice system is constitutional, the fact that the http://wildorchiday.da.ru web site no longer contains child pornography [*see* ¶ 367 above] indicates that the continuing blocking by Comcast of thousands of web sites as a result of Informal Notice 2383 serves no governmental purpose whatsoever.

10. June 2003 – 331,066 or More Web Sites Hosted by the .da.ru Web Hosting Company, Blocked by the Epix.net ISP

370. In addition to sending Informal Notice 2383 targeting http://wildorchiday.da.ru to Comcast on June 11, 2003 (as discussed in the preceding subsection), the OAG also sent Informal Notice 2384 targeting the same URL to the Epix.net ISP. [*Compare* Jt.Exh. 9, Tab B,

line 110 *with* Jt.Exh. 9, Tab B, line 111]. Because both Comcast and Epix.net used IP filtering to comply with their respective Informal Notices, [Jt.Exh. 9, Tab B, lines 110-11], Epix.net also blocked access to the same hundreds of thousands of lawful web sites to which Comcast blocked access.

11. June 2003 – 505 or More Web Sites Hosted by the .pe.kg Web Hosting Company, Blocked by the Comcast ISP

371. In June 2003, as a result of Informal Notice 2386, the ISP Comcast blocked access to a web server of the .pe.kg web hosting company, at the IP address 211.233.3.146, thereby blocking access to at least 505 web sites, at least 502 of which remain blocked as of the trial in this case. [*See* paragraphs immediately following].

372. On June 11, 2003, the OAG issued Informal Notice 2386 to the Comcast ISP, directing Comcast to block access to http://wildorchiday.pe.kg. [P.Exh. 101A (Informal Notice); Jt.Exh. 9, Tab B, line 113 (listing Notice 2386)]. As a result of that Informal Notice, Comcast on June 18, 2003, blocked access to IP address 211.233.3.146. [P.Exh. 101A; Jt.Exh. 9, Tab B, line 113].

373. Plaintiffs' expert Michael Clark researched a list of 505 web sites believe to be at the IP address 211.233.3.146 in November 2003 to verify whether they remained at that IP address as of January 24, 2004. Using DNS lookup tools, Mr. Clark was able to determine that 502 of the web sites shared the IP address 211.233.3.146 as of January 24, 2004. [P.Exh. 101B; Tr. 1/28/04 pp. 13-16 (M.Clark)].

374. Comcast confirmed in its deposition that all of the IP address blocks that it instituted in response to an Informal Notice remained in place as of October 23, 2003. [Dep. of G.Lipscomb (Comcast) at 107].

375. Although Michael Clark's research only verified that certain web sites that existed in October and November of 2003 are blocked, OAG technical staff member Dennis Guzy Jr. confirmed that additional .pe.kg domain names created more recently are also blocked by Comcast. According to his testimony, just before trial Mr. Guzy created a *new* .pe.kg web site, and immediately was able to confirm that the newly created web site was blocked.   [Tr. 1/12/04 pp.53-55 (D.GuzyJr.)]. Thus, in addition to the web sites that Plaintiffs have been able to established are blocked by Comcast, any recently created .pe.kg web sites are also blocked.

376. P.Exh. 95 provides an example of the constitutionally protected content blocked as a result of Informal Notice 2386:

- http://withjesus91.pe.kg (a student's religious-oriented site)

[P.Exh. 95]

377. For the web site listed above, Alexander Roszko explained in his Verification (P.Exh. 95) how he was able to access the web site through the services of the ISP DCAnet, but he was unable to access the web sites when he attempted to access it through the ISP Comcast (which was the recipient of Informal Notice 2386). Instead of gaining access to the web site, the web browser displayed the following message:

> **This page cannot be displayed**
>
> The page you are looking for is currently unavailable. The Web
> site might be experiencing technical difficulties, or you may need
> to adjust your browser settings.

[P.Exh. 95].

12. June 2003 – 505 or More Web Sites Hosted by the .pe.kg Web Hosting Company, Blocked by the Epix.net ISP

378. In addition to sending Informal Notice 2386 targeting http://wildorchiday.pe.kg to Comcast on June 11, 2003 (as discussed in the preceding subsection), the OAG also sent

Informal Notice 2387 targeting the same URL to the Epix.net ISP. *Compare* Jt.Exh. 9, Tab B, line 113 *with* Jt.Exh. 9, Tab B, line 114. Because both Comcast and Epix.net used IP filtering to comply with their respective Informal Notices, [Jt.Exh. 9, Tab B, lines 113-14], Epix.net also blocked access to the same hundreds of lawful web sites to which Comcast blocked access.

13. July 2003 – Laura Blain's Web Sites and Probably Thousands of Other Web Sites, Blocked by the Epix.net ISP

379. As discussed in detail in Section IX.B, above, in early July 2003 as a result of Informal Notice 2545, Epix.net blocked the IP address for Laura Blain's two sites as well as thousands of others.

14. High Likelihood of Other Not-Yet-Identified Blocked Web Sites

380. Plaintiffs have only been able to research a portion of the Informal Notices. Based on the foregoing litany of blocked sites, it is highly likely that additional sites have been blocked but not yet identified. For example, Plaintiffs do not know how Microsoft MSN and certain other smaller ISPs complied with the Informal Notices (and thus what sites might have been blocked). Verizon blocked (through its third party vendors) more than 100 IP addresses, but Verizon could not identify those addresses. Comcast was not able to match up IP addresses with approximately 40 Informal Notices. If fully investigated, any of these situations might reveal blocked sites.

381. Furthermore, Verizon itself recognized the likelihood that it blocked other legitimate sites not identified in an Informal Notice that it does not know about. (Dep. of S.Lebredo (Verizon) at 106-08].

382. There were also times that large numbers of innocent sites would have been blocked if ISPs had not objected. For example, AOL told the OAG that it would not block two large web

hosting companies – GeoCities.com and Trafficgizmo.com – for which it received Informal Notices in 2002 and 2003 because of the massive number of innocent sites that also would be blocked. [Dep. of C.Bubb (AOL) at 136-37; Jt.Exh. 9, Tab B, Lines 208-10, 446].

D. Value of Redirection Sites

383. OAG technical staff member Dennis Guzy Jr. testified that some of the blocked sites above were "redirection sites," [Tr. 1/12/04 pp.47-55 (D.GuzyJr.)], in which a web site owner creates a second web site that incorporates the content from the first web site. Mr. Guzy testified that even if the OAG blocked access to the URL of the second web site, the same content was available by entering the URL of the first web site. [*Id.*].

384. The use of redirection sites is a common, legitimate Internet technique that users often do not even notice. In many cases, a user does not "know anything about the site [he is] being redirected to. . . . [I]n many cases, the name of that site, the URL itself, is extremely cryptic and, therefore, [one] would have no way of accessing where [one] thought [one] was trying to go." [Tr. 2/26/04 pp. 12-13 (M.Marcus)].

385. On cross examination, Mr. Guzy acknowledged that redirection sites can be used to create a "short and pithy" URL for a web site that would otherwise have a long and complicated URL, and that there is nothing wrong or illegal with such redirection sites (assuming the content of the site is lawful). [Tr. 1/12/04 pp.159-60, 173 (D.GuzyJr.)]. During cross-examination, Mr. Guzy visited a number of web sites – with lawful and fully constitutionally protected content – that used short URLs to display content that also resides on other web sites with longer URLs:

- http://chrisenglish.da.ru, a web site of a classical guitarist, with the same content as http://www.edda.freeserver.co.uk/chrisweb/index.html. [Tr. 1/12/04 pp.162-64 (D.GuzyJr.); P.Exh. 86];

- http://ieclub.da.ru, a web site of an English club, with the same content as http://home.uic.tula.ru/~aclub/main.htm. [Tr. 1/12/04 pp.167-68 (D.GuzyJr.); P.Exh. 87]; and

- http://dalmation.da.ru, a web site of an Ohio family, with the same content as http://home.thirdage.com/Pets/dalmation/. [Tr. 1/12/04 pp.169 (D.GuzyJr.); P.Exh. 88].

386. With all three of these web sites, there is absolutely nothing on the "da.ru" version of the web site that indicates that the URL is anything other than the "da.ru" web address. [*See* left-hand screen shots for P.Exhs. 86, 87, 88]. For example, closely reviewing the web site located at http://chrisenglish.da.ru (the left-hand screen shot of P.Exh. 86), there is nothing to indicate that the web site can be located on a different URL. Thus, even someone who had previously visited the http://chrisenglish.da.ru web site would have no way to know how to access the web site after it was blocked by Comcast.

387. Indeed, as seen in P.Exh. 90, the Defendant himself has created two distinct "entrances" to his own web site. The Defendant has created http://www.attygen.net as a second "entrance" to his web site, which is found at http://www.attorneygeneral.gov. [Tr. 1/12/04 pp.170-71 (D.GuzyJr.); P.Exh. 90].

388. If a redirection site is blocked, many people who wish to visit the site will not be able to access it because they will not know what the other URL is, and in many cases will not even know that the other URL exists. [*See* preceding paragraphs].

E. Impact on Individual URLs

389. Section 7622 requires ISPs to "remove or disable access to child pornography items residing on or accessible through its service," and Section 7626(4) requires an application for a

court order to specify the "Uniform Resource Locator providing access to the items." The statute

does not discuss or account for the fact that (as detailed in ¶¶ 53-55 above) a URL only provides

an ephemeral reference to Internet content, and the content displayed by a given URL today may

change by tomorrow. [*See* Jt.Exh. 1].

390. The fact that the Statute and the Informal Notices in actuality only outlaw speech on

a particular location (rather than being narrowly targeted to alleged unlawful speech), is

illustrated by looking at any given Informal Notice. For example, because the Defendant

believed that content located in June 2002 at "www.stopx.com" contained child pornography, the

Defendant issued Informal Notice 1537 to America Online, Inc. (AOL) seeking to permanently

prevent access to any speech of any kind, at any point in the future, at the Internet location

"www.stopx.com." Specifically, Defendant's order to AOL required that "[a]ccess to uniform

resources locator www.stopx.com be denied to your subscribers to your services from an address

located within the Commonwealth of Pennsylvania." As seen in P.Exh. 28A, however, that web

site no longer exists (the "server could not be found"), and Special Agent Dennis Guzy Sr.

agreed that there is no reason to maintain a blocking order against this URL. Nevertheless, AOL

continues to be under an obligation to block access to that URL. [P.Exh. 28; Jt.Exh. 9, Tab B,

Line 410; Tr. 1/9/04 pp.104-09 (D.GuzySr.); P.Exh. 28A; P.Exh. 74 ¶ 7].

391. The permanent banning of URLs that at one time contained child pornography, but

do not any longer, is apparently one goal of the OAG, which stated in discovery responses that

blocking access to a site because it displayed child pornography "in the past" serves a

governmental interest. [P.Exh. 75 ¶¶ 5,7-9, 11, 13, 15, 19, 22].

392. In fact, the OAG specifically told AOL that the Informal Notices do not expire in response to a concern raised by AOL that continuing to add to a permanently blocked list of IP addresses would eventually raise problems. [Dep. of C.Bubb (AOL) at 140-41].

393. With no exceptions shown in the evidence other than where specific complaints about blocked innocent content have been raised to the ISP, the ISPs have continued to maintain in place the technological blocking actions taken in response to the blocking orders in this case. For example, WorldCom continues to block IP addresses as a result of the statutory order it received. [Tr. 1/27/04 pp.99-100 (M.Krause)]. Comcast confirmed in its deposition that all of the IP address blocks that it instituted in response to the Informal Notices remain in place. [Dep. of G.Lipscomb (Comcast) at 107]. AOL also 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].

394. Yet web site content can change frequently. To illustrate the problem, a review of blocked web sites conducted by Michael Clark reveals that almost 30 percent (45 web sites of a sample of 156 web sites blocked by AOL and Comcast) of the web sites no longer exist at all. [P.Exh. 6;Tr. 1/8/04 pp.6-12 (M.Clark)]. Nevertheless, as far as the Statute is concerned (as implemented with the Informal Notices), those 45 web sites remain permanently banned in Pennsylvania.

395. Specifically, the Statute lacks any provision for any subsequent or continuing review of the content located at the referenced URL to determine whether the content available at a given URL in fact continues to be child pornography. [*See* Jt.Exh. 1].

396. Another site that no longer exists is www.lolitasbed.com, whose IP address Comcast blocked in response to Informal Notice 8566, and the Defendant concedes that there is

no governmental interest that is served by the IP address block that Comcast is continuing to maintain. [P.Exh. 74 ¶¶ 4-5; P.Exh. 75 ¶ 6].

397. Among the other web sites that no longer exist (but which continue to be blocked) are http://www.century-sex.com, http://www.teen-teen.biz, and http://www.photo-angels.com. [P.Exh. 6].

398. In addition to the 45 web sites that no longer existed at all (among the 156 Mr. Clark tested), 100 of the web sites tested resolved to different IP addresses than when they were first blocked.[16] [P.Exh. 6;Tr. 1/8/04 pp.6-12 (M.Clark)]. At least some of these 100 domain names no longer contain any child pornography. [*See* following paragraphs.]

399. 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 why that URL should remain blocked. [Tr. 1/9/04 pp.99-101 (D.GuzySr.); P.Exh. 25A]. Yet that URL was the subject of Informal Notice 3529 issued to AOL in May 2002, [P.Exh. 25], was blocked by AOL [P.Exh. 74 ¶ 2], and AOL continues to be obligated to block access to that URL. Similarly, that same domain name was also the subject of Informal Notice 5373 issued to Earthlink [Jt.Exh. 9, Tab B, line 354], and Earthlink remains obligated to block access to the URL (and thus the constitutionally protected speech located at that URL).

400. Plaintiffs' expert Michael Clark explained that this same web site, www.myfirstundressing.com, is now located at a different IP address than the one blocked by AOL in response to Informal Notice 3529, and Defendant admits that is true. [P.Exh. 74 ¶ 3 (Def. Response to Request for Admissions)]. Thus, it is now accessible through AOL's service.

---

[16] As Defendant's expert Ben Stern acknowledged, a change of IP address would be consistent with the scenario in which the original user of a domain name ceased using it and relinquished control over the domain name. [Tr. 2/18/04 p.31 (B.Stern)].

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 pp. 190-93 (M.Clark)].

401. Similarly, although Informal Notice 1711, issued to AOL in August 2002, continues to be in force requiring AOL to block access to http://www.lolitas.unfound-galleries.com, [P.Exh. 30], Special Agent Guzy admitted that the content at that URL does not contain any child pornography and he knew of no justification to continue blocking access to the content located at that URL. [Tr. 1/9/04 pp.101, 104 (D.GuzySr.); P.Exh. 30A].

402. The "www.little-angels.tv" is another example of a URL that is subject to an Informal Notice, but no longer contains illegal content. In addition, www.little-angels.tv illustrates the added difficulty caused by the great flexibility of the Internet and its domain name system, in which a wholly unrelated web publisher can acquire a domain name without any idea that the domain was previously perpetually outlawed in Pennsylvania. To illustrate the problems caused by blocking orders against URLs, and because a portion of the transcript of Michael Clark's testimony concerning www.little-angels.tv was lost due to a tape malfunction, *see* Tr. 1/28/04 p.46-47 (M.Clark), the following is a recap of the relevant facts concerning the URL:

- The URL http://www.little-angels.tv/tr was the subject of Informal Notice 4391, issued to AOL on November 4, 2002. [P.Exh. 105A]

- On or before November 26, 2002, in response to Informal Notice 4391, AOL blocked access to IP address 209.40.127.3. [Jt.Exh. 9, Tab B, Line 247; P.Exh. 46; P.Exh. 105A; P.Exh. 74 ¶ 12].

- IP address 209.40.127.3 is assigned to Cove Software Systems, a Maryland web hosting company that has a strong policy against child pornography. [Tr. 1/12/04 pp.134-38 (D.GuzyJr.); P.Exh. 93]. The OAG did not, however, contact Cove to ask that http://www.little-angels.tv be taken down – instead, the OAG issued the Informal Notice to AOL.

111

- At some unknown point following November 2002 and prior to the fall of 2003, the www.little-angels.tv web site ceased to be maintained. The then-owner of the domain name stopped maintaining the web site hosted by Cove Software, and did not renew ownership of the domain name. At this point in time, Cove Software ceased hosting www.little-angels.tv, and the domain name itself returned to the full pool of available domain names.[17]

- At the same time as (or before) www.little-angels.tv was returned to the pool of available domain names, Cove Software discontinued the assignment of IP address 209.4.127.3 for use by that domain name. Nevertheless, AOL maintains the block on that IP address today. [Dep. of C.Bubb (AOL) at 140-41].

- During the course of this litigation, Plaintiffs determined that the little-angels.tv domain name was not in use and was available for registration.

- On behalf of Plaintiff CDT, Michael Clark (a) purchased and registered the little-angels.tv domain name using the normal domain name registration process, (b) created a brief web site to be placed at that domain, and (c) arranged with a European web hosting company, 1and1.com, to host the web site for free. [Tr. 1/28/04 pp. 46-61, 66 (M.Clark)]

- The resulting CDT-created web site located at http://www.little-angels.tv can be seen at P.Exh. 104, Tab 14, as well as the 4th page of P.Exh. 92. The web site is currently being hosted on IP address 217.160.226.65. [P.Exh. 105].

These facts concerning the URL http://www.little-angels.tv illustrate that (a) the child pornography content on any given URL or IP address is ephemeral, (b) the statutory or Informal Notice blocking orders are perpetual, and (c) anyone can unknowingly later become the victim of the overblocking from the types of blocking orders challenged here. The perpetual blocking effect of the statutory or Informal Notices can harm future protected expression in at least three different ways:

- If Cove Software re-assigns IP address 209.4.127.3 to a new customer, the web site of the new customer (no matter what the domain name) will be blocked by AOL.

- If AOL were to implement the process of monitoring for changing IP addresses (as WorldCom did in response to its court order), then AOL would be blocking access to

---

[17] The exact details of the demise of www.little-angels.tv are unknown to Plaintiffs, but given the fact that the domain name was in the fall of 2003 available in the pool of unused domain names, it is a certainty that (a) the original domain name owner ceased owning the domain name, and (b) the original web hosting company, Cove Software, ceased hosting the web site.

the new version of www.little-angels.tv, even though that web site contains no child pornography or other illegal content.

- If AOL were to implement DNS or URL filtering (as the OAG advocates), then the new www.little-angels.tv would also be blocked, even though the web site is fully lawful.

403. The harmful impact of the perpetual blocks on a URL and domain name are greatly aggravated by the fact that to date almost all of the blocking orders have been totally secret, with no public notice whatsoever as to what is blocked. As Defendant's expert Ben Stern admitted, (a) the secret blocking of domain names introduces significant problems into the domain name registration process; (b) there is no means within the global domain name system for a future purchaser of an unused domain name to know that the domain name is subject to a perpetual blocking order in Pennsylvania, and (c) an innocent web publisher would pay to register a domain name with no idea – and no way to find out – that the domain was permanently blocked by a major ISP. [Tr. 2/18/04 pp.17-19 (B.Stern)].

F. Impact on Smaller Web Speakers

404. The harmful impact to the speech of publishers on the World Wide Web falls most heavily on small and less well funded speakers, thus undercutting part of what makes the Internet such a powerful medium of mass communication. Many web hosting companies offer to host web sites at no cost or a very low cost, and often host all those sites on a single web server using a single IP address. Many small organizations use these types of low cost or free web sites to maintain a web site on the Internet. [Tr. 1/6/04 pp. 26-30 (L.Blain) (describing creation of free and low cost web sites for two community organizations)].

405. For example, Plaintiff PlantageNet offers two levels of web hosting – a less expensive level where all web sites are hosted under a single IP address (for $20 a month), and a more expensive level where each web site receives its own IP address (for $35 a month). [Tr.

1/7/04 pp.102-03 (J.Smallacombe)]. The customers that can only afford (or choose to only afford) the lower priced service are at greater risk of suffering the collateral damage caused by a blocking order in this case.

406. The greater risk of collateral damage to a smaller, less-well funded speaker is seen in the case of the blockage of hundreds of thousands of .da.ru web sites (as detailed in Section IX.C.9 above). As Defendant's expert Ben Stern admitted, a web publisher that wants a unique URL would have to pay $10 to $35 a year just for the right to use a domain name (such as, for example, "bstern.org"). But if that same publisher were content with a unique *subdomain* (such as "bstern.da.ru"), the publisher could use that subdomain for no charge. [Tr. 2/18/04 pp.63-64, 108 (B.Stern)].

407. Smaller web sites are more likely to share IP addresses and domains with entirely unrelated sites, leaving them more vulnerable to both IP filtering and DNS filtering. [*See* preceding paragraphs].

X. Response of Defendant to the Blockages of Sites

408. As First Deputy Attorney General William Ryan frankly admitted, "[t]he statute we have is imperfect obviously." [Tr. 1/9/04 p.211 (W.Ryan)]. Without an adequate understanding of how content is posted on the Internet, the OAG would not be able to begin to try to avoid blocking innocent content. In fact, the OAG did not even attempt to do so. [P.Exh 73 (Defendant's Answers to Plaintiffs' Third Request for Production of Documents and Interrogatories, at ¶¶ 7-9)].

409. Ultimately, the OAG was unconcerned and irresponsible about the fact that the Informal Notice process was directly causing the blocking of access to constitutionally protected speech on the Internet. The OAG did make a minor adjustment to its enforcement of the Statute

114

(and the Informal Notices), but fundamentally the adjustment did not alter the Statute or cure its constitutional defects. [*See* immediately following subsections].

A. Ultimately the OAG Lacked Concern over Constitutional Problems

410. Throughout the time that the Attorney General implemented the Statute, he was well aware that the Informal Notices and court order would result in blocking innocent web sites because of the technological limitations faced by the ISPs. Ultimately the OAG simply ignored such concerns. [*See* following paragraphs].

411. Although the Statute and the Informal Notices are on their face aimed at child pornography, the Defendant *knew* before sending the first Informal Notice that because of the technological reality of the Internet, the removal of some web sites that he believed contained child pornography would also result in protected web sites being blocked. [Dep. of C.Silliman (WorldCom) at 17-22, 60-61, 115-17; Dep. of C.Bubb (AOL) at 43-47].

412. From before the first Informal Notice was sent, the OAG understood that web sites shared IP addresses, [Tr. 1/12/04 pp.22-23 (D.GuzyJr.)], and thus IP filtering risked the blocking of innocent web sites, [Tr. 1/12/04 p.78 (D.GuzyJr.)]. It also understood from very early on that ISPs were using IP filtering to comply. [P.Exh. 24 (May 17, 2002, compliance letter from Innernet.net stating that it had blocked four IP addresses in response to Informal Notices); Jt.Exh. 8].

413. Special Agent Guzy admitted that he cannot determine by looking at a web site whether it shares its IP address with other web sites. [Tr. 1/9/04 pp.171-72 (D.GuzySr.)]. In any event, the 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. [P.Exh. 73, ¶¶ 7-9, 14-15].

414. Even with the one court order under the Statute, the Defendant *knew* there was a risk that innocent content would be blocked (because the order required WorldCom to block access to the Terra.es web hosting service), and yet the OAG decided to proceed anyway. Instead of ensuring that no innocent sites were blocked (by contacting Terra.es directly), the OAG obtained a court order against WorldCom and then sat back to see what WorldCom did. As OAG senior legal adviser John Burfete said to Dennis Guzy Sr., "[l]et's see how they deal with the web hosting issue." [P.Exh. 82].

415. This risk – that innocent content would be blocked by IP filtering – was confirmed for the OAG as early as June 2002, when one of its Informal Notices led to the blockage of hundreds of thousands of innocent web sites by AOL, [*see* Section IX.C.1, above]. In September 2002 after receiving the order to block Terra.es, WorldCom explained in great technical detail why this kind of blockage occurs, [Tr. 1/9/04 p.26 (J.Burfete); Jt.Exh. 8].

416. In September 2002, the AOL ISP also specifically protested to the OAG that Informal Notices targeting Terra.es would block a huge number of web sites, but the OAG continued to send Informal Notices directed at Terra.es after AOL raised those concerns. [P.Exh. 31; Jt.Exh. 9, Tab B, Lines 430, 433; Dep. of C.Bubb (AOL) at 73-82].

417. On October 4, 2002, Special Agent Guzy reported to his colleagues that he had recently spoken with a supervisor at the Lycos/Terra Abuse Unit (located in the United States), who said he would take immediate action if any further child pornography sites were identified on the Lycos or Terra.es system. Special Agent Guzy agreed that the OAG would contact him directly if such a situation arose. [P.Exh.37]. Nonetheless, the OAG sent out two Informal Notices for Terra.es sites that very same day. [Jt.Exh. 9, Tab C, Lines 163, 165 (Informal Notices 3779, 5221 to AOL].

418. In November 2002, Stewart Baker of the U.S. Internet Service Provider Association again explained in detail to the OAG the technical and legal defects in the law and Informal Notice process, and how it was ultimately ineffective. [P.Exh. 14].

419. In July 2003, OAG legal adviser Burfete confirmed yet again that he was aware that IP filtering could lead to the blocking of innocent sites when he spoke to Susan Butchko-Krisa of Epix.net about the blockage of Laura Blain's web sites. [P.Exh. 57].

420. The OAG's response was to reject or ignore those concerns. [*See* paragraphs immediately following].

421. In response to concerns raised by ISPs about the significant overblocking resulting from the Informal Notices, then Executive Deputy Attorney General William Ryan told ISPs at a November 2002 meeting that "it was acceptable damage" and "[t]hat was just the way it was going to have to be." [Dep. of C.Silliman (WorldCom) at 117]. The OAG also expressed that it was ISPs' "obligation under the Statute to implement the blocking as demanded in the informal letters and they were not persuaded at that point about the overbreadth . . . that one IP address or URL might have blocked an entire web hosting service or a service unrelated to child pornography." [Dep. of C.Bubb (AOL) at 97-98].

422. The Attorney General went so far as to assert that blocking innocent sites served its purpose in combating child pornography. According to the Attorney General, if an ISP disabled access to web sites that did not contain child pornography "incidental to disabling access" to a site that did contain child pornography, that "incidental disablement could serve" the governmental purpose of the Statute. [P.Exh. 75 ¶ 2].

423. Members of the OAG told ISPs that they liked the Statute in its current form because it allowed them to go to one place, the ISPs, rather than having to pursue investigations

and legal processes to find the hosts of child pornography sites themselves. [Dep. of C.Bubb (AOL) at 105-06].

424. As late as February 2003, nearly a year after the OAG had first been informed about the particular dangers of blocking online communities, it issued Informal Notices to Verizon, AOL and Erols for a subpage of the GeoCities.com online community, one of the largest in the U.S. [Jt.Exh. 9, Tab C, Lines 290, 319, 325 (Informal Notices 1643 (Erols), 1648 (AOL), 1647 (Verizon))]. Verizon and AOL again had to inform the OAG of the dangers of blocking a site with such a large percentage of legitimate services and businesses. [Dep. of S.Lebredo (Verizon) at 98-99; Dep. of C.Bubb (AOL) at 136-37].

425. After Plaintiff CDT started raising constitutional concerns about the Informal Notice system of Defendant, a senior official in the OAG contacted a number of ISPs to pressure them to "call off the dogs" at CDT. [Dep. of C.Bubb (AOL) at 112-17; Dep. of C.Silliman (WorldCom) at 118-21].

B. The Minor Adjustment in Enforcement Neither Amended the Unconstitutional Statute Nor Avoided its Impact

426. By October 2002 the OAG had begun to admit – internally – that enforcement of the Statute was resulting in massive overblocking of lawful content. The OAG did make a minor adjustment in its procedures, but the adjustment was not successful in avoiding continued massive overblocking. [*See* following paragraphs].

427. In late August and early September 2002, AOL received a series of Informal Notices targeting subpages of the Terra.es web hosting service. [Jt.Exh. 9, Tab A, Lines 31, 40, 42, 45, 54; Dep. of C.Bubb (AOL) at 75]. Christopher Bubb of AOL contacted Deputy Chief Burfete to express his concern about blocking the very large Spanish web hosting service, and was told that it was AOL's responsibility to block the site, and that the OAG did not have the

resources to research every site – even though Mr. Bubb had understood from prior conversations with the OAG that it would not send out Informal Notices for large web hosting services. On September 12, 2002, AOL wrote a follow-up letter to William Ryan of the OAG protesting that Informal Notices targeting Terra.es would block a huge number of web sites. [P.Exh. 31; Dep. of C.Bubb (AOL) at 73-81].

428. Although Special Agent Dennis Guzy Sr. concluded on September 13, 2002, that the OAG would never "be able to figure out all of the web hosting companies," [P.Exh. 32; Tr. 1/9/04 pp.70-71 (D.GuzySr.)], three days later he told his subordinates that he would be responsible for identifying web hosting companies, [P.Exh. 33]. Yet in those intervening three days the OAG had taken no action to be able to identify web hosting companies. [Tr. 1/8/04 pp.77-80 (J.Burfete)]. Agent Guzy Sr. said that he would try to identify web hosting companies "as best I could," [Tr. 1/9/04 p.71 (D.GuzySr.)], although Agent Guzy did not have an accurate understanding of the term "web host." [Tr. 1/9/04 pp.13-14 (J.Burfete)].

429. Notwithstanding the specific concerns that AOL had raised about the risk of blocking innocent content hosted by the Terra.es web hosting company, on October 4, 2002, the OAG sent Informal Notices 3779 and 5221 to AOL instructing AOL to block access to a Terra.es URL. [P.Exh. 41]. At the time this notice was sent, the OAG understood that AOL's compliance with the notice would lead to the blocking of access to 500,000 web sites. [Tr. 1/8/04 pp.99-100 (J.Burfete)].

430. "Starting in October 2002, the OAG began to use a different informal procedure with regard to content located on certain web sites that [Special Agent] Guzy determined were of a kind where the content was posted as a subpage on a web hosting service's web site (*see* Jt.Stips. 18-20 [¶¶ 89-91] above). When one of the agents found a site that the agent concluded,

and [Special Agent] Guzy concurred, displayed child pornography, and the site was a subpage of one of these web hosting service sites identified by [Special Agent] Guzy, 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].

431. Nonetheless, the OAG was unable to avoid blocking innocent sites. Nine of the 13 instances of blocked sites set forth in Section IX.C, above, occurred after October 2002. In addition, at least two times after the OAG started to try to avoid blocking innocent sites, blocking orders were sent concerning two large web hosting companies – GeoCities.com and Trafficgizmo.com – and massive blocking was avoided only because the ISPs refused to comply with the blocking orders. [Dep. of C.Bubb (AOL) at 136-37; Jt.Exh. 9, Tab B, Lines 208-10, 446; P.Exh. 46].

XI. Additional Factual Arguments Advanced by the Parties During the Litigation

A. Theoretically Possible Alternate Methods of Compliance

432. The Defendant's theory of how ISPs should comply with Informal Notices and blocking orders under the Statute has shifted a number of times during this litigation. From early in the Informal Notice process until a few weeks before trial in this case, the OAG has asserted that DNS filtering was the best method for ISPs to use. [*See* Jt.Stip. 33, ¶ 164 above].

433. Plaintiffs, however, contended that both IP filtering and DNS filtering were constitutionally deficient. For the first time in the report of Defendant's expert, Ben Stern, submitted in December 2003, the Defendant advanced a new possible method, URL filtering, that Mr. Stern suggested ISPs could use to comply with a blocking order. [Tr. 1/29/04 (B.Stern) at 17-19]. Later in December (after the deposition of Mr. Stern), the Defendant again shifted,

arguing that URL filtering was perhaps an option that *smaller* ISPs could use. Def. Mem. at 56-57. Then, at trial, Mr. Stern suggested that ISPs could rely on the fact that their corporate customers might already use filters on their own networks. [*Id.* at 75-77]. On top of all of this, the OAG has also asserted that an ISP need not implement any technological blocking action (which the Statute clearly contemplated), but could "contact the host."

434. As made clear in legal briefs, Plaintiffs believe that what is relevant is what the ISPs actually did, not what they might theoretically be able to do. Defendant's solutions would work only in a hypothetical world of far more advanced technology and limitless funds, and under a Statute worded quite differently than the one before this Court.

1. URL Filtering

435. During the course of this litigation, Defendant proposed that ISPs could comply with blocking orders using a technique known as "URL filtering." As Defendant's expert witness Ben Stern admitted, however:

- no ISP has ever implemented URL filtering as Defendant advocates;

- no ISP has ever conducted the extensive investigation and testing into the impact URL filtering would have on the ISP's network and its performance;

- no one known to Mr. Stern (including Mr. Stern himself) has ever conducted such testing; and

- Mr. Stern knows of no "reliable and useful" report or analysis that would assist an ISP (or the Court) in assessing whether URL filtering would work within an ISP's network.

[Tr. 1/29/04 pp.20-22 (B.Stern); Tr. 3/1/04 pp.131-32 (B.Stern)].

436. URL filtering would require an ISP to place a device, or in some cases configure an existing "router" or other device, in the ISP's network to (a) reassemble the packets for most or all Internet traffic flowing through its network, (b) read each http web request, and (c) if the requested URL in the web request matched one of the URLs specified in a blocking order, discard or otherwise block the http request. [Tr. 1/7/04 pp.34-35 (M.Marcus); Tr. 2/26/04 p.6 (M.Marcus)].

437. No ISPs known to either Plaintiffs' or Defendant's experts utilize "URL filtering" to screen all World Wide Web traffic (as the Defendant would require). [Tr. 1/6/04 pp.130 (M.Marcus); Tr. 1/29/04 pp.20-22 (B.Stern); *see also* Tr. 1/7/04 p.84 (J.Smallacombe); Dep. of C.Silliman (WorldCom) at 166; Dep. of G.Basham (Epix.net) at 27-28].

438. Defendant's expert Ben 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 has. [Tr. 1/29/04 pp.20-22 (B.Stern); Tr. 2/18/04 pp.67-68 (B.Stern)]. In Mr. Stern's estimation, any implementation of URL filtering would be a "medium" to "high" level of implementation difficulty. [Tr. 2/18/04 pp.68-69 (B.Stern)].

439. Mr. Stern also admitted that most ISPs do not have the hardware or software required to implement URL filtering. Focusing on financial cost, Stern estimates that the cost of any implementation of URL filtering would be "medium" to "high." In addition to the cost of any additional hardware or software to be purchased, URL filtering would very likely require ISPs to pay continuing "per user" licensing fees. [Tr. 2/18/04 pp.69-72 (B.Stern)].

440. The cost of specialized router hardware that can do URL filtering well runs in the tens of thousands of dollars. [Tr. 1/7/04 pp.53-54 (M.Marcus)].

441. URL filtering also would "significantly degrade the performance of [an ISP's]

network." [Tr. 1/6/04 p.123 (M.Marcus)]. 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.

This degradation of the network manifests itself in the reduction of the capacity of the network to

carry traffic. The filtering task will slow down each switch and router substantially, which

lowers the overall capacity of the network substantially. [Tr. 1/6/04 pp.122-27 (M.Marcus); Tr.

2/26/04 pp. 5-6, 32, 50-51 (M.Marcus)].

442. "Routers" are devices (made by companies such as Cisco and Juniper) within an

ISP's network that "route" or direct Internet communications traffic toward its destinations.

Some routers have the capacity to do URL filtering. If a router has a certain level of capacity, or

through-put, to carry a volume of Internet traffic *without* URL filtering activated on the router,

the capacity is reduced when URL filtering is activated. In this case, an ISP would face two

choices – the ISP could provide poorer, slower service to its customers, or it could buy more

routers. [Tr. 1/6/04 pp.127-29 (M.Marcus); Tr. 1/7/04 pp. 50-51 (M.Marcus)].

443. Specifically, using the Cisco or Alteon devices which are specially designed for

content management (as suggested by Defendant's expert Ben Stern) to conduct URL filtering

would reduce the capacity of a switch by a factor of twenty, *e.g.*, from 100,000 connections per

second to 5,000 connections per second. [Tr. 2/26/04 pp. 8-11, 54 (M.Marcus)].

444. Defendant's expert Ben Stern acknowledges that URL filtering can have a

substantial negative impact on the performance of an ISP's network. Mr. Stern estimates that the

performance impact of URL filtering would be "medium" to "high." [Tr. 2/18/04 pp.72-75

(B.Stern)]. As Mr. Stern admits, even a single URL filter would likely impact performance, and many URL filters would have a greater impact. [*Id.* at 87.]

445. Implementing URL filtering therefore presents significant financial costs to ISPs. First, they would have to purchase new software and hardware to implement the filtering itself. Second, they would have to purchase substantially more switches and routers to maintain the network's prior level of capacity because the switches and routers can handle so much less traffic if they are performing URL filtering. But even if money were no object, URL filtering would degrade the network because technology does not exist today that can do URL filtering at the rate needed to maintain current network speeds. [Tr. 2/26/04 pp. 5-7, 32, 45-48 (M.Marcus)].

446. As compared to IP filtering (which does not significantly degrade the network), URL filtering would be much more harmful to network performance. [Tr. 1/6/04 pp.129-30 (M.Marcus)].

447. The degradation of an ISP's network would occur with both small and large ISPs. [Tr. 1/7/04 pp.36-37 (M.Marcus)].

448. Testimony from ISPs confirmed that URL filtering could not be implemented without significant time and money, and would still result in substantial performance degradation of their networks. [*See* following paragraphs].

449. AOL engineer Brooke Patterson explained that to undertake URL filtering for all AOL members would require significant cost and investment, including development, installation, new hardware and software, management costs, performance assessments, audits, the effect on AOL's existing caching systems, customer support, and further re-engineering of the network. And it would take years to implement. [Dep. of B.Patterson (AOL) at 66-67, 75-

76, 181-87]. It would likely create visible delays in AOL members' Internet experience. [*Id*. at 164-65].

450. Although in the April 2002 meetings Dennis Guzy Jr. asserted that AOL could use its "parental controls" as a form of URL filtering, [Tr. 1/12/04 p.107 (D.GuzyJr.)], on cross examination Mr. Guzy acknowledged that the parental controls service is not effective over the AOL service if the customers use a non-AOL browser such as Internet Explorer. [Tr. 1/12/04 pp.103-04 (D.GuzyJr.); *see also* Dep. of C.Bubb (AOL) at 129].

451. AOL members might use a non-AOL browser for any number of reasons. The AOL browser does not support some advanced web sites; it compresses images; and other browsers have different capabilities and functions that an individual might want to use. [Dep. of B.Patterson (AOL) at 195-96, 198].

452. Furthermore, only a very small subset of AOL customers uses parental controls; the vast majority of AOL customers obtain general Internet access. The ramifications of extending parental controls to the entire AOL customer base would be "far-reaching" and "extraordinarily expensive." It would require AOL to rework its service and invert its business model. [Dep. of C.Bubb (AOL) at 129, 173-75]. Mr. Patterson explained that AOL's parental controls are engineered, architected and scaled to handle only a certain percentage of AOL's traffic. It could not perform filtering for all AOL member traffic. In addition, it only affects members who are using the AOL browser, and the current definition of "effectiveness" for AOL's parental controls is very different than what would be required to ensure compliance. [Dep. of B.Patterson (AOL) at 60-63].

453. Epix employee Gary Basham testified that he "briefly" considered URL filtering but quickly determined that it was too expensive to implement and administer. He knows of no

ISPs that are using filtering technology globally for their entire network. [Dep. of G.Basham (Epix) at 27-28].

454. Verizon engineer Richard Hiester testified that he did not even consider URL filtering an option because of Verizon's network architecture and the time frame in which ISPs were required to comply with Informal Notices. He said that given enough time, it might be possible to implement but it would still not be able to handle all of Verizon's traffic. It would "chok[e] the bandwidth" and have a negative impact on customers. For Verizon to install that across its entire network, it would cost "well into seven figures." [Dep. of R.Hiester (Verizon) at 81-83].

455. WorldCom senior engineer Mark Krause testified that WorldCom would not consider using URL filtering to comply with a future blocking order for two main reasons:

> Because we do not currently have the capability to perform this
> level of filtering on our network [], either because the functionality
> is just not available on the equipment we have, or in the rare cases
> that that type of functionality is available, turning that on would
> cause severe impact on our network and severe performance
> degradation.

[Tr. 1/27/04 p.20 (M.Krause)]. Only a "very very small" amount of WorldCom's equipment could perform URL filtering. [*Id.*]. Moreover, doing the level of URL filtering advocated by the Defendant in this case would require "tremendously more processing power" (as compared to not doing the filtering). [*Id.*].

456. Prior to his testimony Mr. Krause "took a very close look at all of the vendor solutions" mentioned in the Defendant's expert's report. [Tr. 1/27/04 p.19 (M.Krause)]. Those vendor solutions generally only can process a million bits per second "at the top speed" while many of WorldCom's customer connections operate at 48 times that rate. [*Id.* at 20-21]. URL

filtering would require "dramatic hardware changes to [WorldCom's] network in order to think about turning this type of technique on . . . ." [*Id.* at 21].

457. Mr. Krause summarized the inherent unworkability of URL filtering: "The current state of the technology from the vendors doesn't allow us to [implement URL filtering] on . . . our network, based on the types of circuits we have and the speeds [] the circuits are running at currently." [Tr. 1/27/04 p.82 (M.Krause)]. Even if "money were no object" – an obviously unrealistic scenario for any business – WorldCom could not implement URL filtering because the current URL filtering products (a) cannot support the speeds needed in WorldCom's network, (b) do not connect to the type of physical wiring (such as fiber optic and coaxial copper cable) that WorldCom uses, and (c) do not utilize the underlying protocols (such as frame relay, ATM, SONET) that WorldCom uses. [*Id.* at 21-22, 87-89].[18]

458. Mr. Krause estimated that implementing URL filtering in WorldCom's network would require "dramatic" redesign and re-architecture of the network, which would require at least a doubling of the computer and network resources in the network. This in turn would require a doubling of the infrastructure (more building space, more power, more air conditioning, more "rack space") to support the new network equipment. [Tr. 1/27/04 pp.22-23 (M.Krause)]. In all, Mr. Krause estimated that it would require thousands if not tens of thousands of additional routers, switches, and additional "network elements" (with hundreds or thousands of new network elements required to cover just Pennsylvania). [*Id.* at 24-25].

459. None of the products identified by Defendant's expert Ben Stern in his expert report would work in the network of a large ISP because of performance limitations. None of the

---

[18] And, as Mr. Krause made clear during the Defendant's cross-examination of him, WorldCom is not in the business of manufacturing routers, and could not build a manufacturing plant to make specialized routers that would enable large ISPs to comply with blocking orders from the Pennsylvania Attorney General. [Tr. 1/27/04 p.88 (M.Krause)].

identified products can handle anything near the capacity that WorldCom provides to some of its customers – capacity that can be as high as OC-48, or 2.5 billion bits per second. [Tr. 1/27/04 pp.27-28 (M.Krause)].

460. Defendant's expert Stern admitted that the degradation of performance would be particularly acute for ISPs that offer to customers very high speed "optical cable" connections such a OC-12 and OC-48 access. [Tr. 2/18/04 pp.74-75 (B.Stern)]. Mr. Stern's former ISP employer, Allegiance, offers OC-12 service to customers, [*id.* at 75].

461. WorldCom would have difficulty using URL filtering even on traffic of its slower speed DSL customers, because it outsources some DSL services and at times a DSL provider will "aggregat[e] hundreds of thousands of connections onto one very large connection" before delivering the traffic to WorldCom. [Tr. 1/27/04 pp.43-44 (M.Krause)]. Similarly, in less populated markets WorldCom may advertise local services, but in fact contract with the local phone company to aggregate the traffic before delivering it to WorldCom. [*Id.* at 44-45]. *See generally id.* at 61-63 (describing aggregation of traffic at edge routers).

462. Mr. Krause expressed the opinion that there might exist technology that could be used by some (but not all) of "the very smallest of ISP[s]" to do URL filtering. He explained that router vendors such as Cisco make different "flavors" of their hardware and software, with different "feature sets" depending on whether they are targeted to the enterprise market (to be used in an office environment) or to the ISP market. Cisco has implemented URL filtering only in two feature sets targeted at the enterprise market. The ISP-oriented feature sets do not have the URL filtering capability. The enterprise-targeted routers can connect to the type of physical wiring common in office environment, but cannot connect to the wiring typical in an ISP environment. So, a very small ISP might be able to use URL filtering if (a) the ISP could

128

operate using an enterprise-targeted feature set instead of an ISP-targeted feature set, and (b) the ISP's network used common office wiring instead of wiring that is common in an ISP environment. Some ISPs might meet these criteria, but even some very small ISPs could not. [Tr. 1/27/04 pp.83-86 (M.Krause)].

463. Senior technical manager Michael MacDonald of Pennsylvania Online testified that URL filtering would require significant research and testing. [Tr. 1/27/04 p.152 (M.MacDonald)]. Pennsylvania Online is "not capable of implementing URL filtering. We do not have the requisite software or hardware in order . . . to implement that approach . . . ." [Tr. 1/27/04 p.133 (M.MacDonald)]. Mr. MacDonald concluded that in order to be able to implement URL filtering, Pennsylvania Online would need to purchase specialized hardware because attempting to use its existing hardware would cause an unacceptable increased load on the network and would degrade performance. [*Id.* at 133-34]. Although he would need to conduct actual testing of equipment to know for sure, Mr. MacDonald estimated that it would cost Pennsylvania Online at least $20,000 (and possibly much more) to implement URL filtering. An investment of that magnitude would represent a significant percentage of Pennsylvania Online's available capital. [*Id.* at 134-36].

464. If Pennsylvania Online were to invest money to purchase a device capable of performing URL filtering, that investment would not enable the company to add customers or expand its business. The device would exist only to facilitate compliance with blocking orders from the Defendant. [Tr. 1/27/04 pp.158-59 (M.MacDonald)].

465. Because Internet access is a very competitive marketplace, an unrecoverable capital expenditure and a negative impact on performance would have a harmful affect on an ISP's financial success. [Tr. 1/27/04 pp.136-38 (M.MacDonald)]. AOL also believes that

performance is an important element in AOL's competitiveness. [Dep. of B.Patterson (AOL) at 186]. Defendant's expert Ben Stern admits that, because of the competitive marketplace, URL filtering could lead to loss of customers for an ISP, or an increase in expense. Moreover, the introduction of URL filtering into an ISP's network could lead to the violation of "service level agreements" that ISPs have with their customers. [Tr. 2/18/04 pp.77-79 (B.Stern)].

466. ISPs that outsource the Internet access service their customers receive (such as the Plaintiff PlantageNet) would have no way to implement URL filtering because the Internet traffic does not flow through physical devices that are under the ISP's control. Such an ISP would have to pay the wholesale access provider to do the URL filtering, or pay to have all of the ISP's customers' traffic passed back to the ISP so the ISP could attempt to implement URL filtering. [Tr. 1/7/04 pp.95-96 (J.Smallacombe)].

467. Even if PlantageNet's customers' traffic already flowed through its network, that ISP does not have any equipment that is designed to do URL filtering, and PlantageNet's owner, James Smallacombe, expressed serious concern about the adverse impact URL filtering might have on the speed of the traffic passing through its network. [Tr. 1/7/04 p.95 (J.Smallacombe)].

468. URL filtering can also be easily circumvented by simple to implement techniques such as the use of specialized non-standard "port numbers." Typically web traffic travels only to one of three ports: 80, 8000 and 8080. URL filters review traffic going only to those ports, so it can be easily circumvented simply by sending web traffic to a different port. While it is possible to configure a URL filter to review traffic to all ports, that would make the network degradation substantially larger because it would slow down all traffic flowing through a switch rather than just web traffic. [Tr. 2/26/04 pp. 11-12 (M.Marcus); Tr. 2/18/04 pp. 80-85 (B.Stern)].

469. Mr. Stern also identified other specific problems and limitations with URL filtering, including that URL filtering (a) cannot block access if a web site uses the secure https protocol, and (b) cannot block access if the user is using an encrypted anonymous proxy server. [Tr. 2/18/04 pp.80-85 (B.Stern)]. Brooke Patterson of AOL also indicated concerns about its effectiveness and the ability of users to bypass URL filtering. [Dep. of B.Patterson (AOL) at 80].

2. Relying on Corporate Filtering

470. As detailed above, *see* Section VII.C, the DNS filtering method is not effective in situations where an ISP's customer operates its own DNS server or relies on a public DNS server (a not uncommon situation). Thus, an ISP using DNS filtering to comply with a court order would be subject to criminal sanction for failing to block access to a URL for all such customers.

471. In his direct testimony, Defendant's expert Ben Stern asserted that an ISP in the situation described in the preceding paragraph need not worry about the risk of criminal liability because – according to Mr. Stern – some corporations operate filtering products that limit employees access to objectionable content. [Tr. 1/29/04 pp.75-77 (B.Stern)]. Mr. Stern's theory is that a "large number of [corporate targeted] products exist to perform filtering [and so] there's certainly some sort of market for them, and [so] corporations certainly must buy them." [*Id.* at 77].

472. Not all corporations use corporate filtering products, and an ISP could not reliably or easily determine whether its customers used corporate filtering. An ISP that had corporate customers certainly could not assume that every one of those customers would be using filtering products, [Tr. 1/7/04 pp.47-48 (M.Marcus)], or that the products would successfully filter the particular sites identified in an Informal Notice. From its own experience, [*see* Tr. 1/29/04 p.76],

the Court can take judicial notice of the fact that circumstances do exist where corporate employees have child pornography on their office computers.

473. On cross examination, Defendant's expert Ben Stern acknowledged that not all corporations operate filtering equipment, and an ISP would have no effective way to tell if a corporation was operating such equipment. *See* Tr. 2/18/04 pp.48-49 (B.Stern).[19]

474. The theory that an ISP's customer might block child pornography on the customer's own network is irrelevant to the question of whether an ISP "disable[d] access" to a particular URL that is "accessible through" the ISP's services (as the Statute requires). As a factual matter, if an ISP's business customer blocks access to a particular child pornography URL on the customer's network, then *by definition* the ISP failed to "disable access" to the URL in question for that customer (and thus by definition the ISP would remain subject to criminal penalties). Indeed, Defendant's expert Ben Stern agreed that in this situation the business customer would have "unfettered access" to the child pornography site. [Tr. 2/18/04 p.49 (B.Stern)].

475. In light of the facts that (a) not all companies use corporate filtering products, (b) an ISP has no way to know if their customers do use such products, and (c) the use by customers of corporate filtering products would not alter the ISP's criminal exposure, few ISPs if any would "rely on corporate filtering" as a means to comply with a court order under the Statute.

3. Contacting the Host

476. The OAG has never indicated that "contacting the host" would, standing alone, be adequate compliance with the Statute. [*See* paragraphs immediately following].

---

[19] The trial transcript for the pages cited are filled with transcription errors due to tape malfunctions. Plaintiffs believe that they have accurately restated Mr. Stern's testimony, and that Plaintiffs' restatement of that testimony is consistent with the limited information contained in the transcript pages.

477. When WorldCom took this approach, the OAG specifically rejected it. WorldCom received its first Informal Notice in early June 2002. It determined it was not hosting the material, contacted the National Center for Missing & Exploited Children, and passed the information along to another ISP who was closer to the actual web hosting company. When it notified Special Agent Guzy of its actions, Guzy made clear they were inadequate. He clarified that the OAG never thought WorldCom was hosting the materials, but rather that a WorldCom customer had complained about the site, and it was WorldCom's obligation to block it. During this time, WorldCom attorney Craig Silliman determined that the site was no longer accessible on the Internet generally, so the issue was no longer relevant. [Dep. of C.Silliman (WorldCom) at 44-50].

478. Epix employee Gary Basham testified that in assessing how to comply with Informal Notices, he never considered contacting a web host and asking that it remove illegal content. If a web site contained illegal content, he viewed it as a law enforcement responsibility to tell the host, and believed it was not something that an employee at a private company should be doing. [Dep. of G.Basham (Epix) at 28-29].

479. AOL employee Christopher Bubb testified that he did not view contacting the host as a viable method of compliance because of the risk of liability. Mr. Bubb did not want "my criminal liability rest[ing] on the actions of a third party over which I had no control." If AOL failed in getting a web hosting service to do what it asked, that "would have subjected me to liability – criminal liability under the statute for not having complied with the statute." Rather, he viewed that as the OAG's responsibility, particularly given that the statutory definition of ISP was broad enough to cover web hosting services. [Dep. of C.Bubb (AOL) at 190-91].

480. Comcast employee Gary Lipscomb testified that possibly aside from the context of a web hosting service, he would not have considered contacting the host as a compliance option. He felt that Comcast simply had to comply with the Informal Notice by taking action that was within its control. [Dep. of G.Lipscomb (Comcast) at 45-46].

481. As OAG legal adviser John Burfete admitted, the "contacting the host" method of "compliance" is nowhere in the Statute, and the OAG's current position that "contacting the host" constitutes compliance is not binding on either any future Attorney General nor on any current or future of the 67 district attorneys. [Tr. 1/9/04 pp.20-21 (J.Burfete)].

482. In light of (a) the text of the Statute, (b) the implausibleness of the idea that the Legislature intended the ISPs to place a simple phone call to a web host, and (c) the fact that, to avoid criminal liability, an ISP would in some cases have to rely on an unknown third party to take a certain action, it is reasonable to conclude that many ISPs would not determine that "contacting the host" was a viable method of compliance with a court order under the Statute.

B.   Overall Ineffectiveness of the Technical Compliance Methods

483. As discussed both above and below, the various technical actions taken by ISPs in response to blocking orders in this case have been ineffective on a number of different levels. The blocking actions are inherently ineffective in many cases even without any intentional effort to evade a technical block. Intentional evasive action would make the technical blocks ineffective in most if not all cases.

1. Fundamental Difficulties in Attempting to Block Content in the Middle of the Communication

484. Internet and network security expert Professor Matt Blaze explained at trial three major fundamental difficulties with attempting to block access to specified web sites from within an ISP's network.

485. First, Professor Blaze notes that this type of technical blocking action – undertaken in the middle of the network to resist particular types of unwanted or disfavored communication – usually results in an "arms race" with a cycle of blocking action followed by evasive action, followed by blocking action (and so forth). [Tr. 3/1/04 p.18 (M.Blaze)].

486. Second, the communications sought to be blocked in this case are – purely from a technical perspective – properly formatted and technically correct communications. In other words, the web requests and responses sought to be blocked are using the Internet communications protocols as they were designed to be used. Thus there are no non-standard or mis-formatted communications that an ISP can seek to identify or block. [Tr. 3/1/04 p.18 (M.Blaze)].

487. Third and most critically, both sides of the communications to be blocked want the communications to succeed, and thus have incentives both to avoid any blocks and to cooperate with each other on evasive techniques. Unlike "spam" or network attacks (where the recipient does not want to receive the communication), the child pornography user want to access the web site. [Tr. 3/1/04 pp.20-21 (M.Blaze)]

488. Professor Blaze analogized the technical goal in this case to the effort by the federal government in the 1990's to intercept encrypted data as it travels from the sender to recipient. Both cases have willing senders and willing recipients who want to evade the interfering actions

of governments (in this case to block communications, and in the encryption case to intercept communications). [Tr. 3/1/04 pp.21-23 (M.Blaze)].

489. Professor Blaze explained that the Internet was "designed with an end-to-end principle that emphasizes the client and the server in responsibility for getting traffic through. [Filtering techniques] are very difficult to achieve[] because the internet protocols are designed specifically to help end points get traffic through in the presence of a network that's behaving unreliably" (even if the "unreliability" is the result of an intentional blocking action). [Tr. 3/1/04 p.21 (M.Blaze)]. According to Profesor Blaze, "[a]ny communications system designed with an end-to-end model makes it very difficult for a third party to interfere or intercept in ways that don't have the cooperation of the two endpoints." [*Id.* at 23]. [*See also* Tr. 1/6/04 p.71 (M.Marcus) (discussing end-to-end model)].

490. Fundamentally, Defendant's expert Ben Stern agrees with Professor Blaze that attempting to interfere with communications from the middle of the network simply does not make good technical sense. As Mr. Stern explained:

> I think that from a technical standpoint, an ISP in the middle of the communication is not necessarily the most technically appropriate place to make this request [to block content].

[Tr. 2/18/04 p.91 (B.Stern)]. As Mr. Stern stated on his Internet "blog," this general approach is of "questionable wisdom." [*Id.* at 93].[20]

---

[20] In full, Mr. Stern wrote: "Which brings me to my new gig, it's subcontracting for someone who is subcontracting for someone who is contracting with a small government agency. The actual work is not something I am incredibly proud of, but I don't think I'm doing wrong, I am merely getting a closer look at something that is of questionable wisdom, in my opinion, but that's beside the point, or at least I think it is. . . . Just to be clear, I don't think that my discontentment was with the morality of the situation, my position is fairly straightforward, provide technical advice. I am not advocating a particular course of action, nor am I suggesting doing something infeasible. If the other side cannot deal with what I have to say, then I must have a budding career in keeping my trap shut for money." [Tr. 2/18/04 pp. 93-94 (B.Stern)].

2. Ineffectiveness Inherent in Technical Blocks

491. Certain Internet users will not be affected by any filtering method because of the way their computers are configured or the way they search the Web, for reasons having nothing to do with attempting to evade a block.

492. For example, DNS filtering is inherently ineffective because ISPs have many business and organizational customers that operate their own DNS servers or rely on public DNS servers, and thus would not be affected by any DNS filters imposed by their ISPs. [*See* Section VII.C above].

493. As Professor Marcus explained, the use of anonymous proxy services or anonymizers – which are used by persons seeking to maintain their privacy, often for entirely legitimate reasons – would completely circumvent either 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 pp.134-35 (M.Marcus); *see also* Tr. 1/28/04 pp. 76-79 (M.Clark); Tr. 2/18/04 pp.13-14 (B.Stern); Tr. 1/27/04 pp.33-34 (M.Krause); Dep. of G.Lipscomb (Comcast) at 85-86; Dep. of R.Hiester (Verizon) at 36-37].

494. The ISPs confirmed that the blocking actions they took would be completely ineffective if an individual were using an anonymous proxy service or an anonymizer. [Dep. of G.Lipscomb (Comcast) at 85-86; Dep. of R.Hiester (Verizon) at 13, 35-41].

495. Plaintiffs' expert Mr. Clark empirically tested and established that web sites blocked by AOL could in fact be accessed using the anonymizer "Proxify.com." [Tr. 1/7/04 pp.186-89 (M.Clark); P.Exh. 5 & Attachment C; P.Exh. 106 (showing Proxify.com home page)].

496. Among those who rely on anonymizers are users of child pornography who are actively trying to hide their online identity to avoid investigation and prosecution by law enforcement officials. [*See* Section IV.C above]. Thus, a pedophile seeking to remain

anonymous on the web to avoid prosecution also will be unaffected by an Informal Notice or an order under the Statute.

497. Comcast employee Gary Lipscomb confirmed that anonymous proxy servers are "used for malicious activity in some cases." [Dep. of G.Lipscomb (Comcast) at 85].

3. Ability of Child Pornography Users to Intentionally Evade Technical Blocks Should Blocking Orders Resume

498. Child pornography users also could rely on a number of methods to intentionally circumvent a block placed on a web site. If in the future it became known that ISPs were instituting IP, DNS or URL filtering against child pornography sites, users of child pornography could undertake some basic steps to circumvent any of those blocks. [*See* paragraphs immediately following].

499. As discussed above, using an anonymizing proxy service evades all three forms of filtering. [*See* Sections IV.C, XI.B.2 above].

500. Mr. Clark demonstrated in court how easy it is to use web-based anonymizers. He accessed the all-nettools.com web site, typed a URL into a box identified as "anonymous surfing," and was able to access the desired web site through Anonymizer.com. [Tr. 1/28/04 pp. 76-79 (M.Clark); P.Exh. 107].

501. Mr. Clark also demonstrated how to configure a computer to use a proxy service without going through a web site. By doing a search on Google.com for anonymous proxy servers, Mr. Clark located numerous web sites that list the IP addresses of anonymous proxy servers. By changing the preferences in his browser to allow the use of a web proxy, and typing in the IP address of an anonymous proxy server, Mr. Clark configured his computer to use an anonymous proxy server for web searches. Mr. Clark confirmed that this method of accessing

web sites would circumvent both IP and DNS filtering. [Tr. 1/28/04 pp. 80-83 (M.Clark); P.Exh. 108].

502. Likewise, individuals attempting to evade a DNS filter could point their computers to a DNS server not provided by their ISPs. In configuring a Windows computer, there is a straight-forward choice that is offered to either choose the automatically assigned DNS servers, or assign specific DNS servers manually. [Tr. 1/7/04 p.119 (J.Smallacombe)].

503. Ironically, the AOL service itself also could be used by someone seeking to circumvent a blocking order imposed on another ISP. AOL offers a "bring your own access" service for customers who already have a broadband service provider (such as a DSL or cable modem provider). Because the AOL service creates an electronic "tunnel" between the user and AOL's data center, the user's underlying ISP would not have any ability to identify what web sites the user was accessing. For example, if Comcast blocks access to a URL pursuant to a blocking order, a Comcast subscriber would still be able to access the URL by using the AOL "bring your own access" service. [Dep. of B.Patterson (AOL) at 189-90].

4. Ability of Child Pornography Providers to Intentionally Evade Technical Blocks Should Blocking Orders Resume

504. Individuals operating child pornography sites also could implement a number of measures to circumvent blocking measures taken against their sites. If in the future it became known that ISPs were instituting IP, DNS or URL filtering against child pornography sites, child pornography providers could undertake some basic steps to circumvent any of those blocks. [*See* paragraphs immediately following].

505. Bad actors on the Internet have a past track record of evading filtering and other defensive measures – Mr. Krause likened the fight against bad actors as an "arms race" in which

139

once side develops a technique and the other side designs around the new technique. [Tr. 1/27/04 p.21 (M.Krause); *see also* Tr. 3/1/04 p.18 (M.Blaze) (discussing the "arms race")].

506. As Professor Blaze testified, all three technical methods of compliance discussed in this case – the two used by ISPs, IP and DNS filtering, and the one proposed by Defendant, URL filtering – can be easily circumvented, such that if the operators of child pornography sites choose to take action to avoid blocks imposed by Pennsylvania, those blocks (and thus the entire statutory scheme) would be rendered ineffective. [Tr. 3/1/04 pp.24-25, 34-35 (M.Blaze)].

507. IP filtering could be evaded by operators of child pornography sites by a range of methods, including:

- changing the IP address of the web site frequently enough to evade the ability to block new IP addresses;

- changing links to the web site in advertisements;

- changing links to the web site in search engines;

- changing links to the web site in newsgroups;

- promoting the use of proxy servers by publishing instructions to use such devices or providing a program to automate the configuration of the users' browsers; or

- operating a proxy server for the benefit of their users.

[Tr. 3/1/04 pp.26-28 (M.Blaze)].

508. ISPs' experience confirmed that content on the Internet can move locations easily. At least two ISPs found that the URLs identified in Informal Notices issued to them had changed IP addresses, and subsequently changed the blocked IP address. WorldCom, which was subject to a court order, had a process in place to check for IP address changes. AOL did not, but came across a few such changes itself and through subsequent contact from the OAG. [Dep. of C.Silliman (WorldCom) at 97-99; Dep. of C.Bubb (AOL) at 139, 204-05].

509. With regard to another site whose IP address was blocked by AOL, the OAG had to send a second Informal Notice about that same site because it had become available again to AOL users on a different IP address. AOL responded by blocking the new IP address as well. [Dep. of C.Bubb (AOL) at 142-143; P.Exh. 49; P.Exh. 46 page 2 (showing that AOL instituted a block of two different IP addresses on June 20, 2002, and August 5, 2002, for www.teen-teen.biz)].

510. DNS filtering could be evaded by operators of child pornography sites by a range of methods, including:

- using an IP address instead of a domain name;

- changing a portion of a domain name (such as a subdomain name);

- changing links to the web site in advertisements;

- changing links to the web site in search engines;

- changing links to the web site in newsgroups;

- promoting the use of proxy servers by publishing instructions to use such devices or providing a program to automate the configuration of the users' browsers;

- operating a proxy server for the benefit of their users; or

- operating a DNS server for the benefit of their users (including providing instructions on how to point to a different DNS server).

[Tr. 3/1/04 pp.28-29 (M.Blaze)].

511. Professor Marcus also testified that if a child pornography site sends e-mail messages that contain URLs, and the URLs include IP addresses rather than a domain name, DNS filtering would have no effect in blocking access to the URL. Similarly, if a user clicks on a link containing an IP address, or types in a URL with an IP address, DNS filtering would have no effect in blocking access to the URL. [Tr. 1/7/04 pp.40-41 (M.Marcus)].

141

512. URL filtering could be evaded by operators of child pornography sites by a range of methods, including:

- using the encrypted https web protocol instead of the unencrypted http protocol;

- using a non-standard port number (other than the regular http ports of 80, 8000, or 8080);

- using a non-http protocol such as FTP (file transfer protocol);

- changing links to the web site in advertisements;

- changing links to the web site in search engines;

- changing links to the web site in newsgroups;

- promoting the use of proxy servers by publishing instructions to use such devices or providing a program to automate the configuration of the users' browsers; or

- operating a proxy server for the benefit of their users.

[Tr. 3/1/04 pp.30-32 (M.Blaze)].

513. Others confirmed that URL filtering would be "easy to bypass," including by "obfuscating" a URL so it appears different than a blocked URL. [Tr. 1/27/04 pp.23, 30-31 (M.Krause)]. URL filtering also could be evaded by using a specialized "http" port number, [Tr. 1/7/04 pp.55-56 (M.Marcus)], or by encrypting the traffic, [Tr. 1/27/04 p.33 (M.Krause); Dep. of B.Patterson (AOL) at 175].

514. To communicate with customers about new URLs, access methods, etc., child pornography sites would be able to use the same basic techniques that they use today to communicate with customers, *see* Section IV.B above. For example, although Professor Blaze does not have direct knowledge of the child pornography community, he explained that other sub-cultures on the Internet have networks of newsgroups, bulletin boards, and other techniques for exchanging information. [Tr. 3/1/04 pp.32-33, 66-69 (M.Blaze)]. Professor Blaze explained

that such information distribution could be done "very quickly and very efficiently and inexpensively." [Tr. 3/1/04 pp.89-90 (M.Blaze)]

515. A child pornography site would be able to determine that blocking actions were being used – and therefore circumvention measures were needed – through customer complaints, by watching traffic patterns, or most simply by establishing an account with the ISP in question. [Tr. 3/1/04 pp.32-34 (M.Blaze)]. With an account on the major ISP networks, a child pornography site would be able to learn of a new blocking action very quickly. [Tr. 3/1/04 pp.45-46 (M.Blaze)].

C. The Ephemeral Nature of the Defendant's "Reasonableness"

516. The Defendant's asserted "standard of reasonableness" and other deviations from the language of the Statute (including the suggestion that a non-technological "contact the host" approach would satisfy the Statute) have (as John Burfete admits) no foundation in the Statute and are not binding on any future Attorney General, nor on the 67 Pennsylvania district attorneys or any state judge. [Tr. 1/9/04 pp.19-21, 46-47 (J.Burfete)].

517. Notwithstanding the Defendant's claim of "reasonableness," the Informal Notices continued (a) to require compliance (b) in the form of disabling access (c) within five days. Moreover, although John Burfete told a single ISP that compliance with the Informal Notices was "voluntary," he never conveyed that message to any other ISP. [Tr. 1/9/04 pp.22-23 (J.Burfete)]. Similarly, the OAG did not tell any ISPs when they met in November 2002 that no technical compliance actions were required. [Tr. 1/9/04 pp.166-67 (D.GuzySr.)].

518. To the contrary, First Deputy Attorney General William Ryan told the ISPs at the November 2002 meeting that reasonableness was "no longer the standard"; according to Chris

Bubb of AOL, Ryan "specifically denied that being the standard." [Dep. of C.Bubb (AOL) at 93].

D. Likely Future Method of Compliance Should the Statute Be Upheld

519. As detailed above, IP filtering, when coupled with a tool to monitor for any changes of IP addresses, is an effective way to comply with a blocking order. [*See* Section VIII.C above; *see also* Tr. 1/7/04 pp.15, 49-50 (M.Marcus); Tr. 1/7/04 pp.72-73 (J.Smallacombe); Tr. 1/27/04 p.80 (M.Krause)].

520. According to Mark Krause, if the Statute or Informal Notice process were upheld and WorldCom received a blocking order in the future, the technological method WorldCom would use to comply with the blocking order would be IP filtering. [Tr. 1/27/04 pp.15-16 (M.Krause)].[21]

521. According to senior system administrator Michael MacDonald of Pennsylvania Online, if the Statute or Informal Notice process were upheld and that ISP received a blocking order in the future, the technological method Pennsylvania Online would use to comply with the blocking order would be IP filtering. [Tr. 1/27/04 p.131 (M.MacDonald)].

522. From a technical perspective, weighing performance and other costs, Professor Marcus concluded that it would be a reasonable decision for ISPs to choose IP filtering over URL filtering. [Tr. 1/7/04 p.53 (M.Marcus)].

---

[21] Mr. Krause did state that he thought WorldCom would attempt to "contact the host" to see if the web host would quickly remove the content. [Tr. 1/27/04 p.16 (M.Krause)]. Because the entire theory of "contacting the host" is inconsistent with the statutory language, and is only a creation of the OAG in an effort to minimize (but not eliminate) the unconstitutional impact of the Statute, Plaintiffs do not believe that it is likely that in the face of receiving hundreds of blocking orders, possibly from any of 67 district attorneys in addition to the Attorney General, most ISPs would rely on a "contact the host" approach. In any event, as seen in the WorldCom instance, two of the five web hosting companies did not respond quickly enough within the five-day compliance period, and WorldCom did implement IP filtering. [Tr. 1/27/04 pp.92-93 (M.Krause)].

144

523. Professor Blaze expressed alternate possibilities as to what might in the future happen. He expressed his opinion that if child pornography sites take evasive action to avoid blocks, then none of the blocking actions would be effective. But if the sites do not take such evasive action, Professor Blaze believes that an ISP would use "the most straightforward and least costly technique, which would be IP blocking, since that's the closest to normal network management." [Tr. 3/1/04 p.35 (M.Blaze)].

524. Defendant's expert Ben Stern's opinions also lead to the same conclusion – that weighing implementation difficulty, financial cost, and performance impact, a rational ISP would opt to comply with a blocking order with IP filtering. [*See* following paragraphs].

525. The following table is an overview of the negative impacts that IP filtering, DNS filtering, and URL filtering would have on an ISP, collecting the views of the witnesses discussed above (with references to relevant paragraphs above):[22]

---

[22] This table is roughly modeled on the table found on page 13 of the Expert Report of Defendant's expert Ben Stern (identified but not admitted at P.Exh. 59), which was also reproduced as P.Exh. 117 (also identified but not admitted), but the table more specifically reflects the testimony and evidence referenced by the paragraph numbers and thus is essentially independent of P.Exhs. 59 or 117.

Filtering Technique	Implementation Difficulty	Financial Cost	Performance Impact
IP Filtering	Low: AOL (¶239) Low: WorldCom (¶238,242) Low: Blaze (¶237) Low: Marcus (¶237) Low: Guzy Jr. (¶237) Low: Stern (¶240)	Low: Marcus (¶237) Low: Stern (¶240)	Low: Stern (¶240) Low: AOL (¶239)
DNS Filtering	High: AOL (¶242) High: WorldCom (¶243) Low: Stern (¶245)	High: WorldCom (¶243) Low: Stern (¶245)	Low: Stern (¶245)
URL Filtering	High: AOL (¶449) High: Epix.net (¶453) High: Pa. Online (¶463) High: WorldCom (¶458) Medium to High: Stern (¶438)	High: AOL (¶449) High: Epix.net (¶453) High: Pa Online (¶463) High: Verizon (¶454) High: WorldCom (¶457) High: Marcus (¶445) Medium to High: Stern (¶439)	High: AOL (¶449) High: Verizon (¶454) High: WorldCom (¶455) High: Marcus (¶441-43) Medium to High: Stern (¶444)

526. A simple review of these factors makes clear that few if any ISPs would choose URL filtering over IP (or DNS) filtering. Between those two remaining choices, the ISPs are more likely to opt for IP filtering based on fact that DNS filtering is ineffective for customers that do not use the ISPs' DNS servers. [*See* Section VIII.C above].

E. Significant Characteristics of Statutory Order Process

527. The OAG exercised a higher level of care in obtaining a court order against WorldCom than it did in issuing any of the hundreds of Informal Notices. For example, with the court order against WorldCom, the OAG retained a physician to review the alleged child pornography to ensure that the individuals depicted were minors. OAG did not consult a physician on any of the Informal Notices. [Tr. 1/9/04 pp.35-38 (J.Burfete)]. The purpose of consulting with the physician, according to John Burfete, was to "make certain . . . that the materials that we saw were indeed child pornography." [Tr. 1/9/04 p.43 (J.Burfete)].

528. From start to finish, the process of obtaining the single court order issued against WorldCom took almost two months. [Tr. 1/9/04 pp.35-37 (J.Burfete)]. This compares to the very brief time it would take for the OAG to contact the web hosting company hosting child pornography. [Tr. 1/9/04 pp.38-39 (J.Burfete)]. According to Agent Guzy, the OAG could usually contact the host within 24 hours. [Tr. 1/9/04 pp.87-88 (D.GuzySr.)].

XII. First Amendment-Specific Factual Inquiries

A. Impact on Protected Expression

529. Plaintiffs have easily met their burden of demonstrating that speech has been burdened. [*See* Section IX, above, detailing more than 1.5 million blocked web sites].

B. The Government's Failure to Meet its Factual Burdens

530. As discussed in Plaintiffs' briefing, under applicable First Amendment precedent, the Defendant has two specific factual and evidentiary burdens he must carry. In this case, the Defendant has completely failed to carry either burden.

1. The Ineffectiveness of the Statute and Informal Notices

531. The initial and most critical burden that the Defendant must carry in this case is to affirmatively establish that the course of action taken by the Defendant – here the Statute and its implementation in court and through the Informal Notice process – is in fact effective at furthering the asserted governmental purpose.

532. The Defendant formally identified its governmental purpose in discovery, and two staff members identified related purposes in testimony:

- In response to an interrogatory asking for "the governmental purpose(s) that is/are served by the [Statute]," the Defendant responded: "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." [P.Exh. 75 ¶ 1 (Defendant's Responses to Plaintiffs' Fourth Set of Interrogatories].

- In testimony, Special Agent Guzy asserted that the primary purpose of the Statute is to "protect children." [Tr. 1/9/04 pp.115-16 (D.GuzySr.)].

- In testimony, OAG legal adviser John Burfete stated that the governmental objective for the Statute is "the removal of child pornography from the internet." [Tr. 1/8/04 p.108 (J.Burfete)].

The Defendant has not established, and cannot establish, that either the Statute or the Informal Notice process is significantly furthering any of these purposes.

533. First, as explained above, available blocking technology is easily circumvented, both unintentionally and intentionally. [*See* Section XI.B above].

534. Second, Special Agent Guzy asserted that the primary purpose of the law is to "protect children," [Tr. 1/9/04 pp.115-16 (D.GuzySr.)], yet neither the Statute nor the Informal Notice process provide for any action taken against either the alleged child pornography content itself, or the person(s) responsible for the creation and/or posting of such content. Those individuals are allowed to continue to create new child pornography and post it on the Internet. [18 Pa. C.S. § 7622].

535. Even when the OAG had (1) specifically identified a man in Ohio who posted child pornography on the Internet, and (2) directly communicated with the child pornographer, who in e-mail communications admitted using child "models," the OAG chose not to initiate or participate in any prosecution (by either Pennsylvania or Ohio authorities) of the perpetrator. [Tr. 1/9/04 pp.63-67 (D.GuzySr.)].

536. Third, to the extent the governmental objective for the Statute is "the removal of child pornography from the internet" as stated by John Burfete, [Tr. 1/8/04 p.108 (J.Burfete)], the Statute is utterly ineffective in achieving that goal. Indeed, the entire theory of the Statute and Informal Notice system is to leave the content *on* the Internet, and only block access by a subset of Pennsylvanians to any particular instance of child pornography.

537. Although there are dozens of ISPs that operate in Pennsylvania, the OAG has largely limited its Informal Notice efforts to seven ISPs. At any one time, the OAG subscribes to two or three ISPs to search for child pornography content. At present the OAG maintains contracts with only AOL and Verizon in order to search for child pornography on the Internet. It is thus able to confirm the accessibility of such material on only these two ISPs even though OAG is aware that there are many other ISPs providing access to the Internet throughout Pennsylvania. [Tr. 1/9/04 pp.77-80, 93-96 (D.GuzySr.); Jt.Stip. 31].

538. Fourth, whether or not any Informal Notice might have had a small temporary affect on the ability of users of child pornography to access such content, many of the Informal Notices are having no beneficial effect whatsoever today. For example, the vast majority of all web sites blocked by IP address by AOL or Comcast either do not exist at all today or have moved IP addresses. Of a sample of 156 web sites blocked by AOL or Comcast using IP filtering that were tested by Plaintiffs' expert Michael Clark, over ninety percent (145) no longer use the same IP address, and thus AOL's and Comcast's blocks are completely useless today. Indeed, of the 156 web sites tested, almost 30 percent (45) do not exist at all. Thus, in a substantial number of cases, the existing Informal Notices and blocking orders currently provide no beneficial effect whatsoever – but nevertheless may obstruct access to protected expression. [P.Exh. 6; Tr. 1/8/04 pp.6-12 (M.Clark)].

149

2. The Availability and Effectiveness of Less Restrictive Means

539. In contrast to the minimal impact of the Informal Notices on the distribution of child pornography, there exist a number of less restrictive alternatives that would be both more effective and have little if any harmful impact on protected expression. The Attorney General has not met his burden of demonstrating that the Statute and Informal Notices are the least restrictive means of meeting its objectives.

a) Enforcement of Existing Laws

540. The Defendant can, working with Pennsylvania district attorneys, prosecute those responsible for the alleged child pornography, and work with local, federal and foreign authorities to go after child pornography at its source – its producers and distributors. [Tr. 1/8/04 pp.55-56 (J.Burfete)]. The OAG's chief investigator in this matter, Dennis Guzy, has been detailed (while employed by the OAG) to work with local prosecutors on cases involving the sexual exploitation of children. [Tr. 1/8/04 pp.43-44 (J.Burfete)]. Special Agent Guzy detailed in testimony the extensive experience that he has working with local, state, and federal law enforcement on child pornography and exploitation matters (and he remains today appointed as a special detective to Dauphin County District Attorney's Office). [Tr. 1/9/04 pp.113-15 (D.GuzySr.); P.Exh. 72 (D.Guzy resume attached to Defendant's Answers to Plaintiffs' First Set of Interrogatories)].

541. Yet the OAG routinely did not investigate those who created, posted or published the child pornography subject to Informal Notices that it published. [P.Exh. 73, ¶¶1-3]. Thus, even if the child pornography publisher was located in Pennsylvania, the OAG would never know.

b) Cooperation with Law Enforcement Outside of Pennsylvania

542. The OAG also could engage in cooperative efforts with local, federal and international authorities to investigate and prosecute child pornography. As explained in detail in Section IV.A above, such efforts have been successful at finding and stopping child pornographers.

543. Prior to the Statute's enactment, Special Agent Guzy Sr. had worked very closely with federal authorities, including the U.S. Postal Inspection Service and the U.S. Customs Service, on child exploitation issues. [Tr. 1/9/04 pp.54-55 (D.GuzySr.); Section IV.A, above].

544. At a November 2002 meeting with representatives from the OAG, ISPs encouraged the OAG to work with the federal government to go after child pornography at the source, rather than issuing orders to ISPs who did not have the materials on their servers. The ISPs stated that investigating and removing child pornography from the Internet was a law enforcement function. [Dep. of C.Bubb (AOL) at 203-04].

545. Senior OAG legal adviser John Burfete confirmed that there exists no legal impediment to the OAG working with federal authorities to respond to and address alleged child pornography that is located outside of Pennsylvania and even outside of the U.S. [Tr. 1/8/04 pp.55-57 (J.Burfete)].

546. The OAG could become more actively involved in the Internet Crimes Against Children regional Task Force discussed above. [*See* Section IV.A above].

547. The January 2004 indictment in *United States v. Yahor Zalatarou, Regpay Co. Ltd., et al.* ["*Regpay*"] vividly illustrates the value of working with federal and foreign law enforcement with regard to some of the specific web sites targeted by OAG in this case. As part of the larger "Operation Falcon," which coordinates state, local and federal law enforcement

efforts against child pornography, and working in conjunction with law enforcement in Belarus, Spain, and France, *see* P.Exh. 103A at 1-2, the United States obtained an indictment against three individuals and two companies (including the "Regpay" company, also identified in the indictment as "Trustbill") alleged to be responsible for credit card collections for a number of child pornography web sites. Of the five child pornography sites specifically referenced in the indictment, four had been the subject of Informal Notices sent to ISPs. [P.Exh. 103D, at 3]. Those web sites and informal notices include:

Web Site in Indictment	Informal Notices Targeting Same Web Site
www.darkfeeling.com	# 2568 to Comcast (Jt.Exh. 9, Tab B, line 33)
www.juventaclub.com	# 1946 to Comcast (Jt.Exh. 9, Tab B, line 242)
www.lolittles.com	## 1928, 2223 to Comcast (Jt.Exh. 9, Tab B, lines 327-28)
	# 2255 to Epix.net (Jt.Exh. 9, Tab B, line 329)
www.veiledpages.com	# 1864 to Comcast (Jt.Exh. 9, Tab B, line 108)
	# 1460 to Earthlink (Jt.Exh. 9, Tab B, line 453)
	# 1470 to Verizon (Jt.Exh. 9, Tab B, line 454)

Moreover, the Informal Notice process identified numerous other web sites that used the Regpay company for credit card billing, but were not identified in the *Regpay* indictment. At least thirty Informal Notices make direct or abbreviated reference to Regpay (or its a/k/a/ name, Trustbill),[23]

---

[23] The following Informal Notices and URLs reference Regpay or Trustbill, or abbreviations of those names. Plaintiffs are without knowledge as to whether the URLs continue to refer to child pornography, and thus have redacted the domain names. The line numbers are from Jt.Exh. 9, Tab B.

Line No.	ISP	Date of Notice	Notice Number	URL Specified in Informal Notice
59	Comcast	3/25/03	1929	http://www.RedactedURL6.com/trust
60	Earthlink	2/12/03	1674	http://www.RedactedURL7.com/trust/
61	Verizon	2/27/03	1672	http://www.RedactedURL7.com/trust/
62	Comcast	3/14/03	1871	http://www.RedactedURL7.com/trust/
63	AOL	4/4/03	1673	http://www.RedactedURL7.com/trust/
64	Comcast	3/25/03	1934	http://www.RedactedURL8.com/trust
90	Earthlink	2/5/03	1458	http://www.RedactedURL9.com/trust/
91	Verizon	2/10/03	1466	http://www.RedactedURL10.com/trust
92	Comcast	3/14/03	1862	http://www.RedactedURL10.com/trust

and numerous other Informal Notices reference web sites that utilized Regpay for billing services but the reference did not appear in the URL specified in the Informal Notice.[24]

548. Although it cannot be determined at this point in time, had the OAG worked with the federal and New Jersey authorities in conjunction with the Regpay investigation, it is possible that the investigation may have resulted in, at a minimum, arrests of child pornography users in Pennsylvania similar to the 15 Regpay-related arrests made in New Jersey. [P.Exh. 103A]).

95	Comcast	3/25/03	1939	http://www.RedactedURL11.com/regpay
99	Epix	8/6/03	2691	http://www.RedactedURL12.com/rp/
100	Comcast	08/15/03	2703	http://www.RedactedURL12.com/rp/
105	Comcast	3/25/03	1938	http://www.RedactedURL13.com/trust
177	Comcast	3/25/03	1943	http://www.RedactedURL14.com/regpay
187	Comcast	3/25/03	1949	http://www.RedactedURL15.com/trbill
193	Comcast	3/25/03	1927	http://www.RedactedURL16.com/regpay
224	Comcast	3/25/03	1930	http://www.RedactedURL17.com/regpay
233	Comcast	3/25/03	1952	http://www.RedactedURL18.com/regpay
237	Comcast	3/25/03	1953	http://www.RedactedURL19.com/trust
256	Comcast	3/25/03	1954	http://www.RedactedURL20.com/regpay
338	Comcast	3/25/03	1940	http://www.RedactedURL21.com/regpay
349	Comcast	3/25/03	1942	http://www.RedactedURL22.com/regpay
380	Comcast	3/25/03	1951	http://www.RedactedURL23.com/regpay
381	Comcast	3/25/03	1932	http://www.RedactedURL24.com/regpay
456	Comcast	3/25/03	1941	http://www.RedactedURL25.com/regpay
457	Comcast	4/22/03	2117	http://www.RedactedURL25.com/regpay/
467	Comcast	3/25/03	1944	http://www.RedactedURL26.com/regpay
478	Comcast	3/25/03	1937	http://www.RedactedURL27.com/trust
484	WorldCom	7/16/02	5859	http://www.RedactedURL28.com/tb
503	Verizon	2/27/03	1675	http://www.RedactedURL29.com/trust/

[24] Because the OAG was inconsistent in specifying URLs, some Informal Notices referred to URLs with subpages such as "http://www.RedactedURL14.com/regpay" (Informal Notice 1943) while other Informal Notices referenced the same domain name http://www.RedactedURL14.com but without the "regpay" reference (Informal Notice 2125, Jt.Exh. 9, Tab B, line 176). In addition, the actual web pages of the targeted web sites themselves refer to the Regpay billing company (or of its d/b/a name, "RedLagoon"). *See, e.g.,* web pages from sites blocked by Informal Notices 3568, 2704, reproduced in D.Exh. 18. It is difficult or impossible at this point to determine how many of the targeted web sites used Regpay for billing services, but it is clear that the number is well above thirty.

c) Target the Money Flow

549. Another way the child pornography industry can be effectively investigated and prosecuted is by focusing on the flow of money relating to child pornography, and then prosecuting those involved with that money flow. [*See* immediately following paragraphs].

550. Special Agent Dennis Guzy testified that the large majority of the Informal Notices related to commercial, profit-seeking child pornography sites. [Tr. 1/9/04 pp.144-45 (D.GuzySr.)].

551. The *Regpay* investigation discussed above demonstrates the value of "following the money" by investigating how child pornography web sites actually make the money. Beyond the Regpay-related URLs discussed above, there are numerous URLs in the Informal Notices that contain references to other apparent billing entities, for example, "eurobill" and "unionbill." *See, e.g.,* Informal Notices 1459, 2219, 3281 (Jt.Exh. 9, Tab B, lines 204, 334, 345). Moreover, of the 40 web sites surveyed in D.Exh. 18, almost all of them make clear that they are fee-based sites (with statements like "Our site is a paysite," and references to various billing options).

d) Contacting the Host

552. Yet another lesser restrictive means of reaching the government's objectives would be for the OAG to take the more effective and less burdensome approach of directly contacting the entity (usually a web hosting company or ISP) that is hosting the offending web site. The person who places child pornography on the Internet is capable of removing the content from the Internet entirely. [Tr. 1/8/04 pp.39-40 (J.Burfete)].

553. There is ample evidence that contacting the company that is hosting the alleged child pornography content is effective in getting the content removed from the entire Internet (including the Internet as is available in Pennsylvania). The Defendants own expert witness

indicates that web hosting companies usually respond with alacrity to complaints involving child pornography. [Tr. 1/29/04 p.52 (B.Stern)]. A Verizon representative stated that he had never experienced a hosting company's refusal to take down child pornography – "[b]ased on five years of working closely with law enforcement in the . . . Internet community, I've never come across a non-cooperative entity when it came to child pornography." [Dep. of S.Lebredo (Verizon) at 92]. Similarly, WorldCom explained in its deposition that the task of contacting the web hosting company is easy to undertake and appears to be effective most of the time. [Dep. of C.Silliman (WorldCom) at 78-89]. Likewise, Comcast explained in its deposition that it had contacted the host in a couple of scenarios where it was concerned that instituting a block would also block innocent web sites, and that the attempts were successful the two or three times it was employed. [Dep. of G.Lipscomb (Comcast) at 37-38].

554. Based on a conversation he had with a web hosting company, OAG legal adviser John Burfete believes that such companies "would blacklist any KP [child pornography] URL that we advise is KP." [P.Exh. 32]. In September 2002, Burfete told an ISP that "web hosting services upon such contact have removed the offending web site." [P.Exh. 34].

555. Most tellingly, the OAG itself has used this method – *with complete success* – in more than 70 cases. The office even prepared statements of recommended language for telephone contact with Web Hosting Services requesting that they remove posted child pornography. [P.Exhs. 39, 40]. When investigators were given information about a web hosting service that is hosting child pornography, they would contact the host and ask them to remove the offending materials from their service. In *every* instance, the hosting entity promptly complied with the request. According to Agent Guzy, "[t]hey always comply." [Tr. 1/9/04 pp.85-86, 149-50 (D.GuzySr.); Tr. 1/8/04 pp.82-84 (J.Burfete)].

556. As John Burfete, the chief legal adviser to the Defendant concerning the Statute, specifically agreed, contacting the web hosting company would effectuate "the purpose and goal of the act which is the subject of this litigation." [Tr. 1/8/04 p.83 (J.Burfete); *see also id.* at 96-97 (agreeing that contacting the host would "achieve the goals of the law")].

557. According to John Burfete, there is no impediment to the OAG contacting a web host to seek the removal of child pornography. [Tr. 1/8/04 p.99 (J.Burfete)].

558. The information needed to track down the entity to which an IP address has been assigned is publicly available information, and ISPs have no greater access to this information than would the OAG. [Tr. 1/27/04 pp.110-11 (M.Krause)].In fact, 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].

559. The OAG's experience with trying to locate appropriate contact persons indicates that such investigation is within the competency of the OAG staff. OAG technical staff member Dennis Guzy Jr. described at length the techniques he can use to track down a responsible party. [Tr. 1/12/04 pp.57-61 (D.GuzyJr.)]. Mr. Guzy relied primarily on a software tool named "Neotrace" that provides a broad range of information about an IP address, including information gathered from the American Registry for Internet Numbers (ARIN) and its European counterpart (RIPE), which provide information about the ISP, web host, or other entity to which an IP address has been assigned. [*Id.*]. Two other user-friendly web-based tools to obtain information from the ARIN and RIPE databases include all-nettools.com and samspade.org. [P.Exh. 104 Tab 16; Tr. 1/28/04 pp. 68-69 (M.Clark)].

560. The initial search that Mr. Guzy would do to investigate a particular IP address

takes "20 to 30 seconds." [Tr. 1/12/04 p.116 (D.GuzyJr.)]. According to Mr. Guzy, the

information returned about the assignee of an IP address is "very, very accurate." [*Id.* at 116].

561. On cross examination, Mr. Guzy demonstrated through a series of online searches

the detailed types of information available when investigating an IP address. [Tr. 1/12/04

pp.120-43 (D.GuzyJr.)]. The information includes, for example:

- With regard to IP address 207.44.156.52, which was blocked by AOL in response to

  an Informal Notice, [P.Exh. 46, 4th page, ninth line], Mr. Guzy conducted an

  "IPwhois" search on ARIN's web site (www.arin.net) and was able to determine that

  the IP address was assigned to Everyone Internet, Inc., a web hosting company

  located in Houston, Texas. The publicly available information from the ARIN web

  site also provided an "abuse" telephone and e-mail contact for the Everyone Internet

  web host. [Tr. 1/12/04 pp.120-22 (D.GuzyJr.); P.Exh. 91 (screen shot of search);

  P.Exh. 104 Tab 15, 1st and 2nd pages]. A review of the web site of Everyone

  Internet (www.ev1.net) revealed that it offers both web hosting and ISP services. [Tr.

  1/12/04 pp.126-27 (D.GuzyJr.); P.Exh. 91].

- With regard to IP address 81.9.14.98, which was blocked by AOL in response to an

  Informal Notice, [P.Exh. 46, 4th page, sixteenth line], Mr. Guzy conducted an

  "IPwhois" search using the European counterpart to ARIN, RIPE (www.ripe.net) and

  was able to determine that the IP address was assigned to ELTEL.NET, a web hosting

  company located in St. Petersburg, Russia. The publicly available information from

  the RIPE web site also provided an "abuse" e-mail contact for ELTEL.NET. [Tr.

  1/12/04 pp.128-35 (D.GuzyJr.); P.Exh. 92; P.Exh. 104 Tab 15, 3rd and 4th pages]. A

review of the web site of ELTEL.NET (www.eltel.net) revealed that it offers web hosting services, and includes information in English in addition to Russian. [Tr. 1/12/04 pp.134 (D.GuzyJr.); P.Exh. 92].

- With regard to IP address 209.40.127.3, which was blocked by AOL in response to an Informal Notice targeting the domain "http://www.little-angel.tv," [P.Exh. 46, 4th page, tenth line], Mr. Guzy conducted an "IPwhois" search using the ARIN web site and was able to determine that the IP address was assigned to Cove Software Systems, a web hosting company located in Annapolis, Maryland. [Tr. 1/12/04 pp.137-38 (D.GuzyJr.); P.Exh. 93]. A review of Cove Software's web site (which Mr. Guzy stated was a step he would likely do) revealed that the company has an "Acceptable Use Policy" that states:

> We do not allow hosting of Child Porn sites, if a Child Porn site is found on our network the owners will be reported the authorities and the site shutdown. In some cases the sites may remain operational for a short time while under investigation by the authorities.
>
> If Child Porn is found on any other network you may report this to Covesoft as well. We will forward your complaint to our local authority contacts for investigation.
>
> Complaints regarding Child Porn should be sent to security@covesoft.net.

[Tr. 1/12/04 pp.134 (D.GuzyJr.); P.Exh. 93; P.Exh. 104 Tab 17, 2nd and 3rd pages].

562. If a search of ARIN or RIPE for the owner of an IP address does not provide an "abuse" contact, one can be obtained by using an online tool called abuse.net. Abuse.net is a

clearinghouse of email addresses listing the responsible party for domain names. [Tr. 1/28/04 pp. 69-70 (M.Clark);[25] P.Exh. 104 Tab 18].

563. An ISP that is assigned a large block of IP addresses by ARIN (or RIPE, etc.) can in turn sub-assign IP addresses to the ISP's customers. When WorldCom sub-assigns an IP address, it registers the suballocation with ARIN – so that the customer's contact information will appear in response to a IPwhois query. If this customer further suballocates an IP address, that further suballocation might or might not be registered with ARIN. [Tr. 1/27/04 pp.118-19 (M.Krause); Tr. 1/28/04 pp. 155-56 (M.Clark)]. In any event, the information available from ARIN and its counterparts provides a good starting point for determining who is responsible for a particular web server. [*Id.* at 111]. If the information from ARIN does not immediately connect one to the entity responsible for an IP address, it may require a few phone calls to reach the responsible party. [*Id.* at 120-21].

564. This ability to track down a responsible party was proven in practice. With the very first Informal Notice, Dennis Guzy Jr. was easily able to locate the actual web site creator. [Tr. 1/12/04 pp.27-29 (D.GuzyJr.)]. Guzy Jr. was able to locate the responsible individual in "all instances" in which he sought to determine who to call. [*Id.* at 31, 36-37]. Although the OAG sent almost 500 Informal Notices, Guzy Jr. received only "a couple of requests" for this type of investigation. [*Id.* at 29-31].

565. From a technical perspective, as Defendant's expert Ben Stern admitted, all of the risk of collateral damage, financial cost, and harm to performance that are raised by IP filtering, DNS filtering, and URL filtering would be avoided if the OAG "contacts the host" themselves. [Tr. 2/18/04 pp.90-91 (B.Stern)].

---

[25] The transcript from January 28, 2004, contains an error at page 70, line 10. Mr. Clark in fact stated that "The only thing it [abuse.net] will return is email addresses . . ."

566. In light of the foregoing facts, the method of having the OAG "contact the host" is a practical and reasonably effective alternative to the Statute and Informal Notices. Utilizing the approach would avoid the type of blocking of unrelated web sites that has been demonstrated in this case.

XIII.   The Interstate Impact and Significance of the Statute

567. The blocking orders under both the Statute and the Informal Notices have directly halted communications (including a limited amount of illegal communications and a vast amount of lawful communications) that would have otherwise taken place partially and/or wholly outside of Pennsylvania (including communications that would have otherwise taken place wholly outside of the United States). [*See* paragraphs immediately following].

568. ISPs informed the OAG that some ISPs would only be able to implement blocking orders on a nationwide basis. [P.Exh. 9]. Even before the Statute took effect, the OAG Chief Information Officer Peter Sand recognized that the impact of the Statute may well reach outside of Defendant's jurisdiction. [P.Exh. 8, at 2].

569. AOL is "technologically incapable" of confining to the State of Pennsylvania the impact of compliance with blocking orders. [P.Exh. 7]. The blocking actions taken by AOL to comply with the Pennsylvania Informal Notices affect AOL's entire global network, and thus halt communications that would have taken place entirely outside of Pennsylvania (and the U.S.). [Dep. of C.Bubb (AOL) at 125-26].

570. Similarly, the court order imposed on WorldCom under the Statute has directly obstructed communications on WorldCom's entire North American network. [Dep. of C.Silliman (WorldCom) at 20, 97]. Thus, the blocking would affect all WorldCom customers in the United States and Canada, plus 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 pp.107-08 (M.Krause)]. 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 by all users of WorldCom's North American network. [Jt.Exh. 8 p.3].

571. Verizon also told 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." [P.Exh.84, p.2 note 2; Dep. of S.Lebredo (Verizon) at 42-44]. Thus, the innocent content that was blocked for Pennsylvanians when Verizon blocked Terra.es, *see* Section IX.C.2 above, was also blocked for Verizon customers outside of Pennsylvania.

572. As Defendant's expert Ben Stern admits, 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 pp.85-86 (B.Stern)].

573. 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]. Thus, if an AOL dial-up customer in Philadelphia were to access the Philadelphia government's web site, the web traffic would pass through Virginia.

574. Other state legislatures, including in Maryland, New Jersey, and Oklahoma, have considered legislation modeled after the Pennsylvania statute. [P.Exh. 104, Tab 19 (Oklahoma

Senate Bill 755, www.lsb.state.ok.us/2003-04SB/sb755_engr.rtf; New Jersey Senate Bill 2031, www.njleg.state.nj.us/2002/Bills/S2500/2031_I1.HTM; Maryland House Bill 661, mlis.state.md.us/2003rs/bills/hb/hb0661f.rtf)].

575. Blocking orders like those challenged in this case are likely, over the longer term, to directly harm the speed of Internet access available to users. For example, although Comcast uses IP filtering (which has much less harmful impact on performance than the proposed URL filtering), Comcast is increasingly concerned that as more blocking orders come in, the IP filtering is in absolute terms increasing "latency" and slowing down the speed of access for its subscribers. [Dep. of G.Lipscomb (Comcast) at 28-30, 89-94].

576. Over seventeen months the Defendant issued almost 500 Informal Notices affecting about 375 URLs. *See* ¶ 196 above. If this law is upheld, it appears to be reasonable likely that other states will adopt this type of law. If, hypothetically, 20 other states adopt this law, over a two-year period it appears likely that ISPs would be subject to more than 10,000 different blocking orders from 20 jurisdictions. If 40 other states adopt this type of law, over a five-year period it appears reasonable to expect that ISPs would be subject to more than 50,000 different blocking orders. The concern of Comcast (and any other ISP) about the overall harm to its network caused the blocking orders would be radically magnified if instead of receiving about 125 Informal Notices over a seventeen-month period, [Jt.Exh. 9, Tab A, Lines 124-249], it received 12,500 such orders over a five year period. *See* ¶ 576 above.

577. The United States Congress has repeatedly legislated to prevent inconsistent state-by-state legislation affecting the Internet. [S. 877 (108th Cong.), "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" (spam); Internet Tax Nondiscrimination

Act of 2001, Public Law 107-75 (taxation); 15 U.S.C. §§ 6801-6809 (Gramm Leach Bliley Act

pertaining to financial privacy); 47 U.S.C. § 230(c)(1) (content regulation)].

Respectfully Submitted,

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

_____
Stefan Presser, Esq. (SP 120)
Bar No. 43067
Legal Director
American Civil Liberties Union
      of Pennsylvania
125 South Ninth Street
Suite 701
Philadelphia, PA 19107
(215) 592-1513 ext. 116

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

Dated: April 9, 2004