

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

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

**DEFENDANT'S PROPOSED FINDINGS OF FACT
AND CONCLUSIONS OF LAW**

PROPOSED FINDINGS OF FACT

The parties have submitted a Joint Stipulation of Facts. Portions of the Joint Stipulation are incorporated in the following Proposed Findings of Fact by reference. Other portions are paraphrased or referenced where appropriate.

As with Plaintiffs' Proposed Findings, citations are given to materials likely to be in the record, but record citations cannot at this time be complete.

The Parties

1. Plaintiff Plantagenet, Inc. holds itself out to be an Internet Service Provider. However, it does not own the access lines, modems, routers, or other equipment that its customers use when they access the Internet. It has only 750 to 800 customers. Plaintiffs' Answers to First Set of Interrogatories 11, 12.

2. Plantagenet, Inc. has never received an informal notice or notice of court order from the Attorney General under the challenged statute. It has

not shown that it is likely to receive an informal notice or notice of court order in the future.

3. Plaintiff Center for Democracy & Technology has not proven that it has actually been unable to access a web site because of any informal notice or notice of court order issued by the Office of Attorney General under the challenged statute. Plaintiff CDT has not proven that it will likely be unable to access a web site in the future because of an informal notice or notice of court order.

4. Plaintiff ACLU has not proven that it or any of its members have actually been unable to access a web site because of any informal notice or notice of court order issued by the Office of Attorney General under the challenged statute. Plaintiff ACLU has not proven that it or any of its members will likely be unable to access a web site in the future because of an informal notice or notice of court order.

Child Pornography

5. Child pornography as defined at 18 Pa.C.S. § 6312 is not speech.

6. Child pornography as defined at 18 Pa.C.S. § 6312 is not commerce.

7. A determination as to whether an item is or is not child pornography under 18 Pa.C.S. § 6312 is not difficult and can be performed accurately by a law enforcement officer or by a judge acting *ex parte*.

Overview of the Internet and the World Wide Web

8. Joint Stipulation of Facts ¶¶ 6-28 are incorporated by reference.

9. Referencing Joint Stipulation ¶ 7, persons receive content from the Internet through personal computers. These computers can be located pretty much anywhere. These computers are connected to the ISPs' networks as described at Joint Stipulation ¶ 7.

10. Referencing Joint Stipulation ¶ 13, a web publisher may create and have registered any domain name the publisher chooses, so long as it contains a top level domain identifier (*e.g.* .com, .net, .org, .gov, .edu) and is not already registered. The number of possible domain names, and so the number of possible URLs, approaches infinity.

11. Web hosts described at Joint Stipulation ¶ 12 may be layered. That is, one web hosting company may provide server (computer) capacity to another person or entity who functions as a web host to persons who publish web sites.

12. Regarding Joint Stipulation ¶ 25, without a functioning domain name system server assigned in one's computer, one cannot obtain material on the Internet. ISPs give their customers the addresses of DNS servers controlled by the ISPs, and the addresses are entered in the customers' computers during the Internet access set-up process, a process that is often automated.

Implementation of the Statute

13. At or about the time the Internet Child Pornography Law was adopted by the Pennsylvania legislature in February 2002, a group of staff at the Office of Attorney General (OAG) began planning for its administration.

14. In early April 2002, the OAG formed a Child Sexual Exploitation Unit to which it assigned two agents and a supervisory agent. Joint Stipulation ¶ 30. The assigned supervisory agent was Dennis T. Guzy. Mr. Guzy had worked in law enforcement for 25 years, 12 years as a Philadelphia Police Officer, and 13 years as an OAG Criminal Agent. Since 1981, he had specialized in investigation of sex offenses, particularly sex offenses involving children and child pornography.

15. Chief Deputy Attorney General John J. Burfete, Jr. was assigned to be the legal advisor to the Child Sexual Exploitation Unit. Mr. Burfete had been employed by the OAG as a deputy attorney general for 23 years in various criminal law enforcement positions. He reported to Executive Deputy Attorney General William H. Ryan, Chief of the Criminal Division.

16. The implementation planners decided that the OAG objective would be interference with child pornography, not prosecution of ISPs. They decided to be flexible with the ISPs and seek their cooperation.

The Informal Notice Process

17. In March 2002, representatives of several ISPs contacted persons in the OAG and asked for a meeting to discuss implementation of the new law. America Online (Bubb) Dep., p. 26.

18. On April 4, 2002, representatives of the United States Internet Service Providers Association and several ISPs met with representatives of the Office of Attorney General ("OAG") to discuss implementation 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.

19. Both before the April 4 meeting and at that meeting, the ISP representatives stated that they wanted to comply with the law, but also wanted to avoid court proceedings and statutory notices of court orders, which carried a five business day compliance time with possible criminal sanctions for non-compliance. The ISP representatives requested an informal procedure under which the OAG would informally, without a court order, notify them of child pornography items found residing on or accessible through their services, and the ISPs would have the opportunity to remove the items or disable access to them. The OAG staff, which had also been considering some kind of informal approach, agreed to implement an informal procedure. America Online (Bubb) Dep., pp. 19-21, 28-31, 33, 34, 49, 176-78; Verizon (Hiester) Dep., pp. 27-29.

20. The ISPs identified contact persons for the OAG.

21. Mr. Burfete drafted a form of informal notice for the agents to send to the ISPs. Later, around the end of 2002, he drafted the revised form that was used in 2003. Joint Stipulation ¶¶ 35-37.

22. Whether the OAG would or would not proactively search for child pornography, as opposed to only reviewing citizen complaints, was not discussed at either the April 4 or April 15 meeting. At that time, before the law's effective date, no one knew how many citizen complaints the OAG would receive.

23. Starting in late April 2002, after the law became effective, the OAG agents began investigating complaints by citizens regarding child pornography on the Internet. Soon thereafter, the agents began searching 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. Joint Stipulation ¶ 30.

24. 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. Joint Stipulation ¶ 31.

25. 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 Supervisor Dennis T. Guzy reviewed the site and concurred in the conclusion, or when Supervisor 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. Joint Stipulation ¶ 34.

26. The informal notices followed the forms quoted at Joint Stipulation ¶¶ 35-37. They asked the ISPs to remove or disable access to the items identified as child pornography. The notices asked that access be disabled to the ISPs' subscribers who subscribed to the ISPs' services from an address within Pennsylvania. The notices asked the ISPs to remove or disable access to the items within five business days after receipt of the notice and to provide written notice of compliance within five business days after compliance.

27. The informal notices did not coerce the ISPs to disable access to the identified URLs. The notices did not threaten any sanction for failure to respond or comply. No sanction was available for failure to respond or comply. The only procedure available to the OAG upon non-compliance was to file a court application under the statute, 18 Pa.C.S. § 7626. The court application could only lead to an order authorizing the Attorney General to give a formal notice. 18 Pa.C.S. §§ 7627, 7628.

28. The informal notices did not suggest a method by which the ISPs were to remove or disable access to the child pornography items.

29. The OAG's decision as to whether an item was or was not child pornography was made under the standards of 18 Pa.C.S. § 6312. Supervisor Guzy reviewed every site for which an informal notice was sent or court

application filed and determined that it was child pornography as defined at 18 Pa.C.S. § 6312.

30. Throughout their administration of the informal process, the OAG staff liberally allowed the ISPs additional time beyond that stated in the notices to comply, without filing court applications. Specifically,

- a. They gave Microsoft a month after the first notices to it in June 2002 to make arrangements to comply;
- b. In January 2003, they offered America Online and Verizon additional time when they sent out a larger than usual number of notices;
- c. Mr. Guzy told the Comcast representative at the outset that the OAG would work with Comcast as to any time problems, and Mr. Guzy and the other agents gave Comcast additional time throughout the period notices were sent to Comcast, which was predominantly March to September 2003 (Comcast (Lipscomb) Dep., pp. 35, 26, 38, 39, 43).

31. The OAG only filed one court application regarding sites accessed through any ISP, and that one application was made only because WorldCom stated that it would only disable access if required by a court order or other legal process. Joint Stipulation, ¶¶ 44-49, Joint Exhibit 2; WorldCom (Silliman) Dep., pp. 58-64.

32. The court application was filed in September 2002. The court entered its order September 17, 2002. Mr. Burfete sent a Notice of Order to WorldCom the same day by e-mail and overnight mail. Joint Stipulation ¶¶ 45, 46; Joint Exhibits 3, 4, 5, 6.

33. On September 18, 2002, the OAG issued a press release regarding the September 17 order. Joint Stipulation ¶ 47, Joint Exhibit 7. This press release could not reasonably have intimidated ISPs into compliance with informal notices or into any particular method of compliance.

34. WorldCom notified the OAG that it had complied with the Notice of Order. Joint Stipulation ¶ 48, Joint Exhibit 8. The OAG accepted WorldCom's assurances.

35. When ISP representatives expressed concerns about the informal process and the statute, OAG staff met with them, on November 22, 2002. No OAG representative said at that meeting or at any other time that the informal notices had the same force and effect as a court order. See Joint Stipulation ¶ 58.

36. Executive Deputy Attorney General Ryan did contact several ISPs in the Spring of 2003 and asked them to try to get CDT not to pursue a Right to Know Act request that CDT had submitted to the Attorney General. The ISPs told Mr. Ryan that CDT was an independent organization over which they had no control, and Mr. Ryan accepted this response. These conversations had no effect on the OAG's practices regarding the informal notices or the ISPs. The ISPs could not reasonably have interpreted the conversations as threats directed to them.

37. If the Defendant is allowed to resume an informal process of implementing the objectives of the law, OAG staff intends to continue to

administer it flexibly and to consider informal notices issued as requests for voluntary action.

Dealing With Hosts and Publishers of Web Sites

38. In June 2002, Christopher Bubb, an attorney employed by America Online, told Mr. Burfete that he had received a complaint that actions AOL had taken in response to an informal notice had blocked AOL customers' access to some kind of web hosting service and had blocked access to a large quantity of content independent of the child pornography site identified in the notice. He informed Mr. Burfete that the operator of the web hosting service had removed the child pornography item from the service, and AOL had then lifted the block on the service. Mr. Burfete approved of AOL's actions, and so informed Mr. Bubb. America Online (Bubb) Dep., pp. 60-65.

39. Either in the June conversation or other conversations he had with Mr. Burfete over the following several months, Mr. Bubb expressed the view that the OAG should directly contact recognized web hosting services, at least those of the kind that host independent material as subpages on their own domains (see Joint Stipulation ¶¶ 18-20). Mr. Burfete expressed the view that the ISP that received the informal notice should make that contact, and if it did, and if the web hosting service removed the offending material, that would constitute compliance with the informal notice. America Online (Bubb) Dep., pp. 61, 79-81.

40. Mr. Burfete stated his position in the covering letter sent September 17, 2002 to WorldCom with the Notice of Court Order, Joint Exhibit 5.

41. WorldCom reported that it had complied with the Notice of Court Order as to three of the sites identified in it by contacting the entities that hosted the sites who then removed the sites from their services. Joint Exhibit 8. The OAG accepted this method of compliance.

42. Mr. Bubb sent a letter dated September 12, 2002 to Executive Deputy Attorney General William H. Ryan requesting that the OAG itself make the contact with web hosting enterprises like terra.es, where the child pornography item appeared as a subpage on the web hosting site. *see* Joint Stipulation ¶¶ 19, 20.

43. Following receipt of Mr. Bubb's letter, the OAG reassessed its position as to web hosting services, and decided to contact directly web hosting services that permitted independent users to post their content as subpages on the hosting service's site. So, starting around October 2002, when a child pornography item appeared as a subpage on such a site, and when Mr. Guzy recognized that the site was one of these web hosting services, he generally sent an administrator at the service an e-mail requesting that the service take appropriate action regarding the item. In these cases, the OAG agents did not send an informal notice to an ISP through which the child pornography item had only been accessed. Joint Stipulation ¶ 57.

44. If, however, an ISP that received an informal notice itself contacted the host of the child pornography item and the site was removed from the host's services, the OAG continued to accept that action as disablement of access to the item and compliance with the informal notice.

45. If the Court upholds the Statute, or if the Court upholds both the Statute and the informal notice process, Defendant intends to continue the practices set forth in the preceding two paragraphs.

46. ISPs can locate and communicate with other ISPs that host web sites and with other web hosting companies such that when the hosts are told of child pornography on their services, they generally remove it. Verizon (Lebrdeo) Dep., pp. 92, 93, 115-118; WorldCom (Silliman) Dep., pp. 143, 144; America Online (Bubb) Dep., pp. 159-162.

47. However, the ability of a law enforcement agency to locate, communicate with, and gain the cooperation of all kinds of hosts of web sites that display child pornography varies. Except for well-known online communities, some sort of Internet look-up process will be required. This process may not produce the immediate host of the site, but only perhaps the host of the host or some more remote connection. The host may be in a foreign country where communication is difficult. If a foreign host does not cooperate, a state, or even national, law enforcement agency has little real recourse. Verizon (Lebreda) Dep., p. 118; WorldCom (Silliman) Dep., pp. 152-156.

48. Some web sites are published on servers (computers) owned by the publisher, not on servers owned by a web hosting service of any kind and not through any kind of web hosting service. See Joint Stipulation ¶ 11.

49. Law enforcement agencies have little ability to identify, locate, gain the cooperation of, or obtain prosecution of persons who knowingly publish child pornography. No look-up process will easily produce the identity of the publisher of the specific content. The publisher may be in a foreign country. The publisher generally has no desire to cooperate with law enforcement, but rather wants to evade law enforcement.

50. A criminal prosecution of a person who publishes illegal child pornography on the Internet is an expensive, difficult process, particularly when the publisher is located outside the prosecutor's jurisdiction.

51. The Child Sexual Exploitation Unit staff have reported to the National Center for Missing and Exploited Children every case where they identified a child pornography item on the Internet and sent an informal notice to an ISP. The National Center for Missing and Exploited Children is a federal agency that is supposed to forward information regarding possible violations of the federal child pornography laws to appropriate law enforcement agencies. 42 U.S.C. § 13032. The OAG staff have not received any information that any of their reports have led to prosecutions.

52. In the very first case that came to his attention after the law's effective date, Mr. Guzy, with the help of the OAG's Information, Technology, and Law Section, actually was able to identify and contact the operator of the

site where suspected child pornography appeared. The site may have been some kind of online community. The operator was a man in Ohio. Mr. Guzy took this course because the site appeared to be a photo gallery for nudists rather than more typical child pornography, but it did have pictures of nude children. Mr. Guzy believed that direct contact with the site operator was a reasonable way to proceed, if possible, and he was lucky enough to be able to do it. The operator removed the pictures of children from the photo gallery. Although it was a close case, and the operator cooperated, Mr. Guzy still reported the case to the National Center for Missing and Exploited Children.

Methods that ISPs Can Use to Disable Access to Web Sites Not Residing on Their Services

53. The ISPs have used three methods to an effort to comply with the informal notices and the one Notice of Court Order. Joint Stipulation ¶¶ 51-56.

54. First, the ISPs have, on occasion, gone to the host of the child pornography item and requested its removal from the host's services, and, thereby, from the Internet. Joint Stipulation ¶ 56. WorldCom did so to disable its customers' access to three of the sites identified in the Notice of Court Order sent to it in September 2002. Joint Exhibit 8; WorldCom (Silliman) Dep., pp. 78-80, 82, 83. America Online, Verizon, and Comcast have done so as well. America Online (Bubb) Dep., p. 62; Verizon (Lebrede) Dep., pp. 57-59, 115-118; Comcast (Lipscomb) Dep., pp. 36-38, 170-172.

55. Second, some ISPs have used DNS (domain name system server) filtering. Joint Stipulation ¶ 52. Verizon used DNS filtering as its sole method of compliance for its entire former Bell Atlantic network. Epix used DNS filtering at first in conjunction with IP address filtering, but after July 2002, for the last 29 informal notices that it received, it used DNS filtering exclusively. Earthlink used DNS filtering. Verizon (Lebrede) Dep., pp. 15, 16; Epix (Basham) Dep., pp. 10-12.

56. Third, some ISPs have used IP address filtering. Joint Stipulation ¶ 54. America Online used IP filtering exclusively. WorldCom used IP address filtering for two of the sites identified in the Notice of Court Order.

57. Comcast experimented with both DNS filtering and IP address filtering. It decided to use IP address filtering apparently because, due to Comcast's network architecture, it could limit IP address filtering to its Pennsylvania customers, but could only apply DNS filtering nationwide. All of Comcast's IP address filtering applied only to its Pennsylvania customers. Comcast (Lipscomb) Dep., pp. 18-21, 25-28, 109-111.¹

58. In fact, the above three methods are all available today to an ISP to disable access to child pornography items identified in either an informal notice or Notice of Court Order. An additional method, "URL filtering," exists technologically and is feasible on smaller networks.

¹ A Verizon witness testified that he understood that a contractor on the old GTE portion of Verizon's network also chose IP address filtering over DNS filtering because IP address filtering could be limited to Pennsylvania. Verizon (Lebrede) Dep. p. 112.

DNS Filtering

59. DNS filtering is a simple, inexpensive, reasonably effective method of disabling access to web sites, and it poses little risk of disabling access to un-targeted sites. Epix (Basham) Dep., pp. 16, 73; Verizon (Hiester) Dep., pp. 33-35.

60. For DNS filtering, the ISP makes entries in the domain name system servers to which its customers' computers are generally assigned. Joint Stipulation ¶ 53. The entries prevent the "fully qualified domain name" (www.example.com) found in the requested site's URL from resolving to its IP address. Without the IP address of the requested site, the request cannot proceed. The requestor gets a message stating that the request has failed.

61. DNS filtering poses little risk of overblocking. It stops requests only for those URLs that contain the fully qualified domain name for which the entry is made. It does not stop requests for any other sites. It will not even stop requests for subdomains of the domain name; thus if the entry stops requests for "www.example.com," it will not stop requests for www.acehardware.example.com.

62. DNS filtering stops requests for all subpages under the fully qualified domain name entered. Therefore, if the fully qualified domain name included in the URL is of an online community that allows users to post their independent content as subpages on the community site, the DNS server entries will stop requests for all of the pages on the community, not just the page that displays the targeted child pornography item.

63. The OAG policy of going directly to web hosting services (such as online communities) that allow postings as subpages, and the OAG's acceptance of ISPs' direct contact with these kinds of hosting services, largely avoid the limited overblocking potential of DNS filtering.

64. The ISPs' blocking of entire online community sites mostly happened before the OAG began its practice of contacting web hosting services directly in October 2002. America Online (Bubb) Dep., pp. 54, 55, 186; Comcast (Lipscomb) Dep., pp. 49, 50; Verizon (Lebrede) Dep. Pp. 51, 62, 63.

65. DNS filtering is easy for an ISP to implement. It requires no new equipment. It requires little staff time. It has no adverse effect on the ISP's system. Verizon (Hiester) Dep. Pp. 45-47; Epix (Basham) Dep., pp. 16, 73.

66. DNS filtering is an effective method of preventing access to the identified child pornography site. It remains effective so long as the URL, or, actually, the fully qualified domain name, remains the same, even if the site changes its IP address. Verizon (Lebrede) Dep. pp. 124, 125.

67. While computers can be assigned to DNS servers not under the control of the user's ISP, this possibility does not interfere with the ability of DNS filtering to disable access to child pornography.

68. The DNS server assignment process makes use of a different DNS server unlikely. ISPs give their customers the addresses of DNS servers controlled by the ISPs, and the addresses are entered in the customers' computers during the Internet access set-up process, a process that is often automated.

69. Larger businesses that operate their own computer networks often have their own DNS servers and do not use the DNS servers controlled by the ISP through which the business network accesses the larger Internet. Verizon (Lebrede) Dep., pp. 130, 131. However, the computers on these business networks are used by the businesses' employees for business purposes. The employees are not likely to access child pornography over their workplace computers.

70. In the workplace, attempts to access child pornography would likely be discovered, either by casual observance or through organizational network monitoring, with negative repercussions for the employee who accessed the pornography.

71. Filtering products on the market are sold for use by business or organizational networks. Some businesses use them. They will prevent employees from accessing child pornography on the organizational network.

72. A home user can redirect his computer to a DNS server not controlled by his ISP. However, redirection is not something home users are likely to do to any great degree. It requires knowledge that this is possible and knowledge how to accomplish it. It requires knowledge of the IP address of an alternate DNS server. It requires knowledge of the steps that must be taken to enter that IP address into the user's computer. It requires the stomach to change the configuration of one's computer, particularly for something as essential as domain name system service. Verizon (Lebrede) Dep., pp. 118, 119, 130, 131.

73. The OAG has accepted DNS filtering as compliance with the informal notices.

74. At the meetings in April 2002, the ISPs and OAG staff discussed methods of disabling access to sites accessible through, but not residing on, an ISP's services. Representatives of the OAG advanced the use of DNS filtering as a possible method that ISPs could use to comply with informal notices.

Joint Stipulation ¶ 33.

75. Verizon's compliance letters in response to informal notices consistently stated that Verizon was using DNS filtering. The OAG never objected. After receiving the first such letter, Mr. Guzy noted to his superiors that Verizon had disabled access via Verizon controlled DNS servers, and that Verizon had followed the recommendations of OAG staff and had done so successfully.

76. In July 2003, after the ISP Epix discovered that its IP address filtering had blocked an untargeted site, it told Mr. Guzy and Mr. Burfete that it intended to use only DNS filtering in the future, and received no objection. Epix (Basham) Dep., pp. 19-23, 57-60, 65, 66; Epix (Butchko-Krisa) Dep., pp. 11-14, 18-22.

77. If the Court upholds the Statute, or if the Court upholds both the Statute and the informal notice process, Defendant intends, based on current technology, to continue accepting DNS filtering as compliance with a notice to disable access to a child pornography item not residing on the ISP's services.

IP Address Filtering

78. IP address filtering (or blocking) is a reasonably simple and effective means of disabling access, but it has downsides, the most serious of which is that it risks substantial overblocking of untargeted sites.

79. IP address filtering involves entries made in routers or switches controlled by the ISP, which entries prevent requests for a particular IP address from leaving the ISP's network. Joint Stipulation ¶ 55. Because IP addresses are today often shared by a number of separate domains, blocking an IP address substantially risks blocking many sites not targeted for blocking. This overblocking risk is much greater than for DNS filtering.

80. In this light, IP address filtering can be useful where the IP address is known to relate to only one site, as is usually the case when the only identifier of the site is the IP address (in which case, it can't be filtered out at the DNS server).

81. IP address filtering can be more time consuming than DNS filtering because it usually requires a look-up process to determine the IP address for the URL in question.

82. Large numbers of IP address blocking entries in an ISP's routers and switches can adversely affect network performance.

83. IP address blocking becomes ineffective if the IP address associated with a particular URL changes, as they often do. A request for the URL will resolve to an IP address that is not blocked, and the request will reach the desired content.

84. In the future, a reasonable ISP faced with an informal notice or notice of court order under the Statute will not generally choose IP address filtering over contacting the host or DNS filtering.

URL Filtering

85. “URL filtering” exists technologically, is feasible on smaller networks, and is effective where it can be used. Products for URL filtering are currently sold aimed at use on organizational networks.

86. To filter outgoing requests for specific URLs, equipment that an ISP either might already be using, such as routers or cache servers, or equipment that an ISP could install in its network, could be configured to perform the filtering. As the requests pass through, or by, the equipment, that equipment can look inside the “packet” to see the URL requested and stop those URLs that have been programmed into a control list.

87. URL filtering filters out URLs right down to the specific subpage. It presents no risk of disabling access to untargeted sites.

88. However, the ability of an ISP to apply “URL filtering” today varies depending on the ISP’s size and architecture. It is possible for smaller ISPs, particularly for those with existing equipment that could accommodate the task. It may become more feasible in the future as ISPs install new equipment.

Anonymizer Proxies

89. The existence of “anonymizer proxies” does not negate the validity of any of the above filtering methods.

90. An anonymizer proxy requires that the user's computer be configured to send all requests for web sites through another computer, the "proxy server." That proxy server then makes the request for the desired web site, and does so stripped of any information that identifies the original requester.

91. Even a person seeking child pornography would not likely use an anonymizer proxy. Use of an anonymizer proxy presents obstacles, costs, and risks. The user must first know that such things exist and must find one. The user must, in all likelihood, pay to use the anonymizer. The user then must learn how to configure his computer to use the proxy. The user must accept the risks of a reconfiguration that sends requests through another computer that the user does not control. The user must trust that other computer, its operators, and whatever software is involved. Even after the user finds the proxy, pays for it, and gets it operating safely, it imposes problems. Making payments by credit card (the only way to pay on the Internet) is difficult when anonymous. Without payment the child pornography cannot be purchased, and the most desired material may not be accessible.

93. Even the Senior Manager of Network Abuse and Policy Observance at Comcast has never used an anonymizer. Comcast (Lipscomb) Dep., p. 112.

The Future

94. The World Wide Web was really just developed in the early 1990's. Both it and the underlying Internet have continued to develop rapidly since

then. The technology of the WWW and the Internet will surely continue to develop and change in the future.

CONCLUSIONS OF LAW

1. Plaintiff Plantagenet, Inc. lacks standing to sue. Defendant's Brief, Arg. I, pp. 9-14.

2. Plaintiffs Center for Democracy & Technology and American Civil Liberties Union have standing to sue on the claims that the Pennsylvania's Internet Child Pornography Law, 18 Pa.C.S. § 7621-7330 (the Statute) creates a prior restraint and lacks constitutionally sufficient procedural processes to determine child pornography. Otherwise, these two plaintiffs lack standing to sue. Defendant's Brief, Arg. I, pp. 9-14.

3. Child pornography, as defined at 18 Pa.C.S. § 6312, has no constitutional protection, as speech or commerce.

4. The Statute is constitutional insofar as it authorizes court orders and notices of court orders directing Internet Service Providers to remove child pornography items residing on their services. Defendant's Brief, Arg. II, pp. 15-17.

5. The Statute does not create any perpetual or ongoing restraint on the use of a URL or IP address if the URL or IP address does not provide access to a "child pornography item." Therefore, the Statute does not create a perpetual or ongoing prior restraint of protected speech. Defendant's Brief, Arg. III.A., pp. 18-20.

6. Even if the Statute authorizes a notice directing continuing disablement of access to a URL after it no longer provides access to a child pornography item, it does not sufficiently restrain protected speech to implicate the First Amendment. Defendant's Brief, Arg. III.B., pp. 20-21

7. Even if the Statute authorizes a notice directing ongoing disablement of access to a URL after it no longer provides access to a child pornography item, and even if that notice truly does impose on protected speech, the imposition is not directed against protected speech, but against child sexual abuse. The imposition does not violate the First Amendment. Defendant's Brief, Arg. III.C., pp. 22, 23.

8. The Statute provides constitutionally adequate procedures, including adversary hearing and proof of child pornography by the State, before any determination of child pornography coerces any restraint on speech. Defendant's Brief, Arg. IV.A., pp. 23-27.

9. Assuming the initial order of authorization under 18 Pa.C.S. § 7627 is coercive, the Statute provides constitutionally adequate procedures before it is issued. Defendant's Brief, Arg. IV.B., pp. 28-39.

10. The Statute does not violate the First Amendment insofar as it authorizes court orders and notices of court orders directing ISPs to disable access to child pornography items accessible through their services. Defendant's Brief, Arg. VI., pp. 45-61.

11. The Statute, and the orders and notices it authorizes, do not violate the Commerce Clause. Child pornography is not commerce. Any

effect the Statute, and its orders and notices, may have on legitimate commerce do not discriminate against interstate commerce. Any effects on legitimate interstate commerce do not burden commerce sufficiently to invalidate the Statute. Defendant's Brief, Arg. VII., pp. 61-66.

12. The informal notice process does not coerce any ISP into disabling access to web site. Therefore, the informal notices do not create any prior restraint, perpetual, ongoing or otherwise; the Constitution does not require that any particular procedures precede an informal notice; the informal notices cannot violate the First Amendment; the informal notices cannot violate the Commerce Clause. Defendant's Brief, Arg. V.B., pp. 42-45, Arg. VI, pp. 50,51.

13. Even if the informal notices do coerce ISPs into disabling access to web sites, the informal notices, like the Statute, create no perpetual, ongoing prior restraint that violates the Constitution; the procedures employed before informal notices are issued comply with the Constitution; the informal notices did not and do not violate the First Amendment; and the informal notices did not and do not violate the Commerce Clause. Defendant's Brief, Args. II, V, VI, VII.

14. The Preliminary Injunction entered September 9, 2003 must be vacated.

15. Judgment must be entered in favor of the Defendant.

GERALD J. PAPPERT
ACTING ATTORNEY GENERAL

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

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

CERTIFICATE OF SERVICE

I, John O. J. Shellenberger, hereby certify that the foregoing Defendant's Proposed Findings of Fact and Conclusions of Law has been filed electronically and is available for viewing and downloading from the Court's Electronic Case Filing (ECF) system. A true and correct copy of the foregoing was mailed on December 31, 2003 by e-mail and first class mail, postage prepaid, to:

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

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

Seth Kreimer, Esquire
3400 Chestnut St.
Philadelphia, PA 19104

GERALD J. PAPPERT
ACTING ATTORNEY GENERAL

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

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