CENTER FOR DEMOCRACY & TECHNOLOGY, On Behalf of Itself; AMERICAN CIVIL LIBERTIES UNION, On Behalf of Its Members; and, PLANTAGENET, INC., On Behalf of Itself and Its Customers, Plaintiffs, vs. GERALD J. PAPPERT, Attorney General of the Commonwealth of Pennsylvania, Defendant.

CIVIL ACTION NO. 03-5051

UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF PENNSYLVANIA

337 F. Supp. 2d 606; 2004 U.S. Dist. LEXIS 18295

September 10, 2004, Decided

. . .

E. ISP COMPLIANCE WITH COURT ORDERS OR INFORMAL NOTICES

. . .

2. Methods of Implementation

108. According to the ISPs, on most occasions, they attempted to comply with the Informal Notices by implementing either IP filtering or DNS filtering. These methods were either used alone or together. Jt. Stip. P 51. 109. Use of IP filtering, DNS filtering, or URL filtering to block content accessible through the service of an ISP only affects Internet users who access the Internet through that ISP's service. Thus, Internet users that do not use the service of an ISP that blocked a web site would still have access to the blocked content. Tr. 1/7/04 (Clark) pp. 183-90.

a. DNS Filtering

110. "DNS filtering" is sometimes referred to as "DNS spoiling" and "DNS poisoning." Jt. Stip. P 52. The Court will use the term DNS filtering to refer to this method of filtering. 111. To perform DNS filtering, an ISP makes [**57] entries in the DNS servers under its control that prevent requests to those servers for a specific web site's fully qualified domain name (found in the requested site's URL) from resolving to the web site's correct IP address. The entries cause the DNS servers to answer the requests for the IP addresses for such domain names with either incorrect addresses or error messages. Without the correct IP addresses of the requested sites, the requests either do not proceed at all or do not reach the desired sites. Joint Stip. PP 52, 53; Tr. 1/29/04 (Stern) pp. 43-45; Tr. 2/18/04 (Stern) pp. 99-100. Def.'s FOF P63.

b. IP Filtering

112. IP filtering is also referred to as null routing. Jt. Stip. P54. The Court will refer to this method as IP filtering.

113. To implement IP filtering, an ISP first determines the IP address to which a specific URL resolves. It then makes entries in routing equipment that it controls that will stop all outgoing requests for the specific IP address. Jt. Stip. P55.

c. URL Filtering

114. Mr. Stern testified that ISPs could comply with blocking orders using URL filtering. This technique was also one of the methods mentioned by Dennis Guzy, Jr. at the [**58] April 2002 meetings with ISPs. Pls.' FOF P 435; Tr. 1/12/04 (Guzy, Jr.) pp. 16-17. URL filtering involves the placement of an additional device, or in some cases the reconfiguration of an existing "router" or other device, in the ISP's network to (a) reassemble the packets for Internet traffic flowing through its network, (b) read each http web request, and (c) if the requested URL in the web request matches one of the URLs specified in a blocking order, discard or otherwise block the http request. Tr. 1/7/04 (Marcus) pp. 34-35; Tr. 2/26/04 (Marcus) p. 6; Pls.' FOF P 436.

3. Comparison of Filtering Methods

a. Ease of Implementation and Cost

115. The ISP market is very competitive and the speed and performance of a [*629] network is an important factor in the public's perception of an ISP. Tr. 2/18/04 (Stern) p. 77. Because the market for Internet access is "very competitive," if an ISP were to implement a [filtering method] which adversely affected [its] network performance . . . [or] if [its] network became slower, it would be added incentive for [its] customers to jump ship." Pls.' FOF P102; Tr. 1/27/04 (MacDonald) pp. 136-38. 116. Most ISPs already have [**59] the hardware needed to implement IP filtering and IP filtering is a fairly routine aspect of the management of a network. IP filtering is used to respond to various types of attacks on a network, such as denial of service attacks and spam messages. Pls.' FOF P 237; Tr. 3/1/04 (Blaze) pp.14-15 (explaining denial of services attacks and spam); Tr. 1/7/04 (Marcus) p. 55. For example, IP null routing (or IP filtering) is something that WorldCom uses "routinely." Pls.' FOF P 237; Tr. 1/27/04 (Krause) pp. 78-80. WorldCom has an automatic system (developed for network management reasons unrelated to Pennsylvania blocking orders) that can implement an IP null route on all of WorldCom's thousands of routers "relatively instantaneously, within a matter of seconds to minutes." Pls.' FOF P 238; Tr. 1/27/04 (Krause) p.52. For AOL, IP filtering is "in common use as a defensive mechanism against such activities as virus proliferation, spam, et cetera. It is a basic and common tool of the trade." Dep. of B. Patterson (AOL) at 38. 117. IP filtering generally does not require ISPs to purchase any new equipment and it does not have any impact on network performance. Pls.' FOF P 239; Dep. of B. Patterson [**60] (Senior Network Administrator for AOL) at 38-40, 52. Dennis Guzy, Jr., testified that IP filtering is "easy to perform" and is indeed the "easiest" method of filtering for an ISP to use. Pls.' FOF P 237; Tr. 1/12/04 (Guzy Jr.) pp. 76-77; Pls.' Ex. 85 (Nov. 18, 2002 memo by Dennis Guzy, Jr.). Most ISPs can implement IP filtering with their existing equipment and many ISPs already have an existing internal procedure to implement IP-based blockage. Tr. 2/18/04 (Stern) pp. 23-24. 118. Most ISPs that do not outsource Internet access would not be required to purchase new equipment to implement DNS filtering. If the ISP's staff is familiar with this method of filtering, the necessary entries in the DNS servers require no expenditure of money and little staff time. Tr. 1/29/04 (Stern) pp. 87-93; Tr. 1/7/04 (Marcus) pp.

17-24; Hiester Dep. pp. 33-35, 45-47; Basham Dep. pp. 16, 73. Almost all ISPs that do not outsource Internet access can utilize DNS filtering for customers that use their DNS servers. Tr. 1/29/04 pp. 67 (Stern); Tr. 1/27/04 (Krause) pp. 68-70; Tr. 1/27/04 (MacDonald) pp. 147-148, 159; Patterson Dep. pp. 15-16, 123-125, 131; Def.'s FOF P 74. 119. DNS filtering would be more difficult [**61] for some ISPs to implement. Compared to IP filtering, as Professor Blaze explained, DNS filtering is a "much more specialized technique" within the network security field. Tr. 3/1/04 (Blaze) pp. 15-16. According to Mark Krause of WorldCom, DNS filtering is "not a very standard process" and "not something that ISPs would normally do." Pls.' FOF P 241; Tr. 1/27/04 (Krause) p. 75. 120. AOL does not currently perform DNS filtering on its network. As of February 3, 2004, AOL would have been required to make entries manually in all of its 100 DNS servers to implement a DNS block. Automating this process would involve designing a new system to do DNS filtering, assessing the related risks, assigning additional long-term staff, and developing auditing and monitoring systems. Dep. of B. Patterson at 47-51, 136-42. [*630] Given these factors, Mr. Patterson said he would recommend IP filtering to AOL; he would not recommend DNS filtering. Id. at 51-52. 121. DNS filtering would "require [WorldCom] to radically redo the way [it] currently implements [its] DNS system to [its] customers." Tr. 1/27/04 (Krause) pp.16-17. WorldCom does not have "a built-in infrastructure to push out configuration [**62] changes to those [DNS] systems" (Id. at 17) and implementing DNS filtering would require WorldCom to purchase and configure additional DNS servers in its network and potentially reconfigure the systems of millions of customers. Id. at 17-18. 122. With the exception of AOL and WorldCom and other ISPs that do not currently perform DNS filtering, the cost of implementing IP filtering and DNS filtering is "approximately equal." Tr. 1/29/04 (Stern) p.128. More generally, the difficulty of implementation, financial cost, and performance impact of DNS filtering and IP filtering are similar. Pls.' FOF P 245; Tr. 2/18/04 (Stern) pp. 46-47. 123. No ISPs known to either plaintiffs' or defendant's experts utilize URL filtering to screen all World Wide Web traffic. Tr. 1/6/04 (Marcus) pp. 130; Tr. 1/29/04 (Stern) pp. 20-22; Tr. 1/7/04 (Smallacombe) p. 84; Dep. of C. Silliman (WorldCom) at 166; Dep. of G. Basham (Epix) at 27-28. AOL performs URL filtering on a portion of its network, but it cannot utilize URL filtering on its entire network at the present time. AOL calls this URL filtering service "parental controls." AOL engineer Patterson explained that to undertake URL filtering for [**63] all AOL members would require expenditures for development, installation, new hardware and software, management costs, performance assessments, customer support, and further re-engineering of the network. It would take years to implement and be "extraordinarily expensive." Dep. of B. Patterson (AOL) at 60-63, 66-67, 75-76, 181-87; Pls.' FOF P 449; Dep. of C. Bubb (AOL) at 129, 173-75; Pls.' FOF P 452. AOL's parental controls are engineered, architected, and scaled to handle only a certain percentage of AOL's traffic; these controls could not perform filtering for all AOL member traffic. Dep. of B. Patterson (AOL) at 60-63. 124. ISPs would be required to develop new equipment and conduct testing with this equipment before implementing URL filtering. For example, an ISP would be required to purchase substantially more switches and routers to maintain the network's prior level of capacity because the switches and routers can handle less traffic if they are performing the computations necessary for URL filtering. Tr. 2/26/04 (Marcus) pp. 5-7, 45-48; Pls.' FOF P 445. Mr. Stern acknowledged that any implementation of URL filtering would require extensive research and testing, and he admitted [**64] that he had not done such testing and did

not know of anyone who had done so. Tr. 1/29/04 (Stern) pp. 20-22; Tr. 2/18/04 (Stern) pp. 67-68. Mr. Stern also admitted that most ISPs do not have the hardware or software required to implement URL filtering. Tr. 2/18/04 (Stern) pp. 69-72; Pls.' FOF PP 438. 125. If an ISP did not purchase substantially more switches and routers, URL filtering would "significantly degrade" the performance of an ISP's network. Tr. 1/6/04 (Marcus) p.123; Tr. 2/18/04 (Stern) pp. 72-75. Such degradation is caused by the fact that the technical process of comparing all of the URLs in the web traffic flowing through an ISP's network with a list of URLs to be blocked is "expensive" in the computational sense - it requires a significant amount of computing power. Performing these computations would slow down each switch and router substantially [*631] and decrease the overall capacity of the network. Tr. 1/6/04 (Marcus) pp.122-27; Tr. 2/26/04 (Marcus) pp. 5-6, 32, 50-51 (M.Marcus); Pls.' FOF P 441. 126. The purchase and testing of the equipment necessary to perform URL filtering would require a significant investment by ISPs. Engineers from Epix, Verizon, Pennsylvania Online, [**65] Plantagenet, and WorldCom all testified that their ISPs do not perform any URL filtering. Dep. of G. Basham (Epix) at 27-28; Dep. of R. Hiester (Verizon) at 81-83; Tr. 1/27/04 (MacDonald - Pennsylvania Online) p. 133; Tr. 1/7/04 (Smallacombe - PlantageNet) pp. 95-96; Tr. 1/27/04 (Krause - WorldCom) p. 20. It would cost Verizon "well into seven figures" to implement URL filtering across its entire network. Dep. of R. Hiester (Verizon) at 83. "Money aside, the current [URL filtering] technology . . . would not be able to even operate in [WorldCom's] network" because the current URL filtering products (a) cannot support the speeds needed in WorldCom's network and (b) do not connect to the type of physical wiring (such as fiber optic and coaxial copper cable) that WorldCom uses. Tr. 1/27/04 (Krause) p. 21-22, 87-89.

b. Relative Effectiveness

127. An ISP's use of DNS filtering does not impact customers that do not use the ISP's DNS servers. Pls.' FOF P 247; Tr. 1/6/04 (Marcus) pp. 115-18; Tr. 2/18/04 (Stern) p. 47. Customers are not required to use the DNS server provided by their ISP. Mr. Stern specifically acknowledged that "large businesses often operate their own [DNS servers]. [**66] " Pls.' FOF P 248; Tr. 1/29/04 (Stern) pp. 68-69. 128. Because DNS filtering is not effective for all of their customers, some ISPs chose not to use this method.

(a) Pennsylvania Online does not require its customers to use its DNS servers and does not know whether any particular customer uses its DNS servers. Tr. 1/27/04 (MacDonald) pp. 145-48. Pennsylvania Online used IP filtering to comply with the Informal Notices it received because it was the "most effective solution to ensure compliance" and because DNS filtering can be "easily circumvented" by customers running their own domain name server. Id. at 131-32; Pls.' FOF P250.

(b) WorldCom did not use DNS filtering for two reasons. First, WorldCom could not easily implement this method for the reasons set forth in Finding of Fact 121. Second, "[DNS filtering] would not allow [WorldCom] to fully comply with the court order . . . due to the fact that not all of [WorldCom's] users use DNS servers under its control." Tr. 1/27/04 (Krause) p. 16. According to Mr. Krause, medium and large businesses often operate their own DNS servers. Id. at 76-77; Pls.' FOF P 251. WorldCom's customer base is primarily businesses and ISPs [**67] (to whom

WorldCom provides wholesale Internet access) that maintain their own DNS servers. Thus, in terms of compliance with a court order, WorldCom "thought that [DNS filtering] simply was so seriously flawed that it was not a workable solution." Mr. Silliman expressed these concerns to the OAG. Pls.' FOF P 252; Dep. of C. Silliman (WorldCom) at 104-06, 110-11, 133.

(c) AOL was concerned that the 67 district attorneys empowered to enforce the Act might not agree with the OAG's opinion that DNS filtering was an acceptable method of compliance. Dep. of C. Bubb (AOL) at 207-08. Furthermore, AOL's users could change their configurations to different DNS servers either manually or by loading applications that do it for them. Additionally, some customers that access AOL using a broadband Internet connection are assigned a different DNS server by the third party providing the broadband [*632] service. Dep. of Patterson at 16, 44-45.

129. Other ISPs informed the OAG they were concerned about the use of DNS filtering because they had customers that did not use their DNS servers and would be unaffected by such filtering. For example, Verizon informed the OAG that not all of its customers used [**68] its DNS servers, and DNS filtering for those customers would not be effective. Pls.' FOF P254; Tr. 1/9/04 (Guzy Sr.) p. 160-61; Pls.' Ex. 84 (Aug. 16, 2002 letter from Verizon to OAG); Dep. of S. Lebredo (Verizon) at 25. Moreover, the Attorney General was on notice of this problem with DNS filtering because the OAG operates its own DNS server. The approximately 1,000 employees of the OAG do not rely on the DNS server of the OAG's ISP, Verizon, and would not be affected by Verizon's use of DNS filtering. Pls.' FOF P 255; Tr. 1/12/04 (Guzy Jr.) p. 72.

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

131. Even a home user can redirect his computer to a DNS server not controlled by his ISP. However, redirection is not something home users who are not actively seeking child pornography are likely to do to any great degree. It requires knowledge that it is possible, an understanding of how to accomplish it, knowledge [**69] of the IP address of an alternate DNS server, and knowledge of the steps, often complicated, that must be taken to enter that IP address into the user's computer. Tr. 1/29/04 (Stern) pp. 80-83; Tr. 1/7/04 (Marcus) pp. 26-29; Tr. 1/7/04 (Smallacombe) pp. 113; Lebredo Dep. pp. 118-119; Hiester Dep. pp. 38-39.

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

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

134. A child pornography web site can evade an IP filter by obtaining a new IP address for the web site. [**70] Tr. 1/7/04 (Marcus) pp. 14-15. A web site's IP address can change without the URL changing. Tr. 1/29/04 (Stern) pp. 62-63, 65. If, however, the ISP implementing the IP filter monitors the web site for a new IP address and changes the IP address being filtered to block the new address, the IP filtering is still effective. Id. at 15. Such a monitoring program is easy to create. Pls.' FOF P 261; Tr. 2/18/04 (Stern) pp. 33-34. WorldCom utilized IP filtering monitors - it "implemented a tool to monitor for any of those [IP address] changes and to alert [WorldCom] to [the change], so that then [it] could go and adjust the null routing to follow the change made in the DNS." Pls.' FOF P 262; Tr. 1/27/04 (Krause) p. 80.

135. Because DNS filtering stops a request for the domain name before it has been resolved to an IP address, it continues to prevent access to the identified child pornography item even if the offending site changes its IP address. Tr. 1/29/04 [*633] (Stern) pp. 62-64; Tr. 2/18/04 (Stern) p. 136; Tr. 1/7/04 (Marcus) pp. 18-19; Def.'s FOF P 65.

136. IP filtering is more effective than DNS filtering because IP filtering blocks content for all users, including those who [**71] do not use DNS servers under an ISP's control. Although a web host can evade IP filtering by changing a web site's IP address - a technique that will not defeat DNS filtering - an ISP can track these changes and block the new IP address. Pls.' FOF P 260; Tr. 1/29/04 (Stern) pp. 127-28; Tr. 1/7/04 (Marcus) pp. 49-50; Tr. 2/18/04 (Stern) pp. 31-32. Thus, it is reasonable for an ISP to chose IP filtering as a method of compliance over DNS filtering.

c. Overblocking

137. DNS filtering stops requests for all sub-pages under the blocked domain name. Thus, if the domain name included in the URL identified by an Informal Notice is of a Web Hosting Service that allows users to post their independent content as sub-pages on the service's site, the DNS server entries will stop requests for all of the independent pages on the service, not just the page that displays the targeted child pornography item. Tr. 1/29/04 (Stern) pp. 50-51; Tr. 2/18/04 (Stern) pp. 103-107. For example, DNS filtering results in overblocking when an online community such as the GeoCities web site, which allows many different users to have web sites on sub-pages of GeoCities.com, is targeted by an Informal Notice. [**72] Pls.' FOF P 285; Tr. 1/6/04 (Marcus) pp. 109-10; Tr. 2/18/04 (Stern) pp. 54-56, 60.

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

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

blocked. Thus, if da.ru was blocked, subdomaina.da.ru and subdomainb.da.ru would also be blocked. Tr. 2/18/04 (Stern) p. 54.

140. IP filtering leads to a significant amount of overblocking. As Mr. Stern stated, IP filtering "will block innocent sites to a great deal," Tr. 1/29/04 (Stern) p. 65, and "IP address [**73] filtering is extremely likely to block untargeted sites due to the process known as virtual hosting," Id. at 128. Dennis Guzy Jr. reached an identical conclusion, stating that it is "very easy to block access to additional sites" when using the IP filtering method. Pls.' FOF P 282; Pls.' Ex. 85 (Nov. 18, 2002 memo from Guzy, Jr.).

141. IP filtering leads to blocking, of innocent web sites, because of the prevalence of shared IP addresses, as detailed in Findings of Fact 16, 42, and 43. If an ISP uses IP filtering to block access to a particular IP address, all web sites hosted at that IP address are blocked. Tr. 1/6/04 (Marcus) pp. 103-04. As an example, in response to Informal Notice 2545, Epix.net blocked access to IP address 204.251.10.203, which in turn blocked access to two of Laura Blain's web sites and others hosted by directNIC. Pls.' FOF P 283; Pls.' Ex. 54 (InformalNotice 2545); Pls.' Ex. 56 (internal Epix.net e-mail indicating [*634] that 204.251.10.203 blocked in response to Informal Notice 2545 and that this was also the IP Address for directnic.com's hosting service).

142. URL filtering filters out URLs down to the specific subpage. It presents no risk of disabling access [**74] to untargeted sites. Tr. 1/29/04 (Stern) p. 102; Tr. 2/18/04 (Stern) p. 106; Tr. 1/6/04 (Marcus) p. 122; Def.'s FOF P 112.

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

. . .

8. Methods of Evasion

a. Anonymous Proxy Servers

197. Internet users who want to keep their identity secret can use anonymous proxy servers or anonymizers. In the context of visiting web sites, these services route all requests through the proxy server or anonymizer, which in turn sends the request [**103] to the desired web site. Requests using these services appear to the ISP routing the request as if they are requests directed to the proxy service, not to the underlying URL to which the user actually seeks access. Pls.' FOF P 132; Tr. 1/6/04 (Marcus) pp. 132-35.

198. The use of anonymous proxy services or anonymizers completely circumvents both of the technical blocking methods - IP filtering and DNS filtering - used by the ISPs to comply with the Informal Notices and would circumvent URL filtering as well. Tr. 1/6/04 (Marcus) pp. 134-35; Tr. 1/28/04 (Clark) pp. 76-79 (demonstrating use of proxy service); Tr. 2/18/04 (Stern) pp.13-14; Tr. 1/27/04 (Krause) pp. 33-34; Dep. of G. Lipscomb (Comcast) at 85-86; Dep. of R. Hiester (Verizon) at 36-37. [*644] For example, web sites blocked by AOL could be accessed through AOL's service using the anonymizer "Proxify.com." Tr. 1/7/04 (Clark) pp. 186-89; Pls.'

Ex. 5 (Third Report and Testimony of Michael Clark) & Attachment C (demonstrating that site was blocked by AOL but that he was able to access it using Proxify.com); Pls.' FOF PP 493-495.

199. If the child pornography seeker chooses to have all of his web requests run through a proxy or anonymizer, [**104] he faces obstacles and risks. First, he must learn how to configure his computer to do so. This requires a number of difficult entries. Second, even if he successfully configures his computer, the seeker must then accept the risks of a reconfiguration that sends all requests through another computer that the user does not control - risks that the connection will not work or that the service will be slow. Tr. 1/29/04 (Stern) pp. 84-87; Tr. 1/7/04 (Marcus) pp. 39-40; Tr. 3/1/04 (Blaze) p. 76.

200. Individuals attempting to evade a DNS filter can do so by manually entering the IP address for a DNS server that is not controlled by their ISP. Tr. 1/7/04 (Smallacombe) p.119; Pls.' FOF P502.

b. The Ability of Child Pornographers to Evade Filters

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

202. IP filtering can be evaded by operators of child pornography sites [**105] by changing the IP address of the web site. Finding 140; Tr. 3/1/04 (Blaze) p. 26. In one instance, the OAG sent a second Informal Notice relating to one site because it had become available to AOL users at a different IP address after AOL blocked the original IP Address. AOL responded by blocking the second IP address as well. Dep. of C.Bubb (AOL) at 142-143; Pls.' Ex. 49 (InformalNotice 9851); Pls.' Ex. 46 page 2 (showing that AOL instituted a block of two different IP addresses on June 20, 2002 and August 5, 2002 for same URL).

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