



Law & Public Policy Department
22001 Loudoun County Parkway
Room E1-3-501
Ashburn, VA 20147
703 886 0700
Fax 703 886 4399

VIA FACSIMILE AND OVERNIGHT MAIL

September 23, 2002

John J. Burfete, Jr.
Chief Deputy Attorney General
Computer Forensics Section
Office of Attorney General of Pennsylvania
2490 Boulevard of the Generals
Norristown, PA 19403

Dear Mr. Burfete:

I am writing in response to the order from the Court of Common Pleas of Montgomery County, Pennsylvania (the "Order") directing WorldCom, Inc. and its subsidiaries that are Internet Service Providers (collectively, "WorldCom") to block access by its subscribers in Pennsylvania to certain Uniform Resource Locators ("URLs") on the Internet. This order was signed on September 17, 2002 and was received by WorldCom, along with notice from the Office of the Attorney General of Pennsylvania, on September 18, 2002. As discussed in detail below, we believe that WorldCom has complied with this court order.

As you know from our previous conversations with your office, WorldCom does not have any relationship to any of the sites listed in the Order. WorldCom does not host any of the sites, nor do we have any other legal or physical control over any of the sites or the content contained in them. Moreover, we would like to reiterate that WorldCom is absolutely opposed to child pornography, and that we regularly work with law enforcement in various jurisdictions to disable access to any child pornography that might temporarily be hosted by WorldCom and to provide evidence to prosecute those responsible.

The Order directs WorldCom to deny access to the following URLs to persons subscribing to WorldCom Internet services from an address within the Commonwealth of Pennsylvania:

1. <http://www.teen-teen.biz>
2. <http://free.bigout.com/gallery.html> also identified as <http://www.free.bigout.com/gallery.html>
3. <http://www.girlsroom.tuportal.com/two/html>
4. <http://love.xloli.com/?lustv.xloli.com>
5. <http://www.terra.es/personal8/jenout/>

In your letter to WorldCom transmitting the Order, you stated that "[o]ne or more of the URL's identified may be to a Web hosting service" and "if the hosting service [removes] the offending web site, and the site is thereby no longer accessible through WorldCom to Pennsylvania residents, you will have complied with the Court Order and Notice."

As noted above, none of the sites represented by the five URLs identified in the Order is hosted by WorldCom; rather, all five sites are hosted by service providers unrelated to WorldCom. In compliance with the Order, subscribers (and other users) of WorldCom's Internet services in Pennsylvania will not be able to access these sites through the WorldCom Internet network. In the case of three URLs, each site has been disabled by the hosting provider. In the case of the other two URLs, WorldCom

cannot be certain that the sites will be disabled by the hosting provider within the five business days mandated by the Court for compliance, so we have begun to block access to the Internet Protocol ("IP") addresses associated with those sites. As discussed in more detail below, the result of compliance with the Order with regard to the two sites being blocked by WorldCom is that all users of WorldCom's North American Internet network (whether those users are located inside or outside of Pennsylvania) will be unable to access any Web sites or other content or services that share the IP addresses of the sites at issue.

Sites That Have Been Removed By the Hosting Providers

The sites represented by the URLs <http://free.bigout.com/gallery.html>, <http://www.terra.es/personal8/jenout/>, and <http://www.girlsroom.tuportal.com/two/html> have each been disabled by the service provider that was hosting the material. These hosting providers are BlueTelegraph.com, Terra.es, and Acens.com, respectively. WorldCom used publicly-available materials to identify the service provider hosting the site in question and we notified that service provider that the Office of the Attorney General had determined that the relevant site contained child pornography. In each case, the service provider immediately disabled the site, and 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.

In addition, a sixth URL, <http://www.terra.es/personal9/xxxwm2002/00000.p.htm>, was listed in your notice letter to WorldCom but was not listed in the Order. Although this URL was not listed in the Order, I wanted to inform you that the hosting service provider has disabled the site represented by this URL.

In conformity with our customary practice when notified of child pornography accessible via our network, WorldCom also reported each of these sites, as well as those discussed below, to the National Center for Missing and Exploited Children, the national clearinghouse for reports of child pornography to law enforcement.

Sites To Which WorldCom Is Blocking Access

With regard to URLs <http://www.teen-teen.biz> and <http://love.xloli.com/?lusty.xloli.com>, WorldCom contacted the hosting provider, and in both cases we were told that the sites would be disabled. WorldCom cannot be confident however, that the sites will be permanently disabled within the five business days the Court has ordered for compliance. As a result, WorldCom has developed a technical solution to block access by users of the WorldCom Internet network in Pennsylvania (and, because of the nature of the technical solution, users located elsewhere) to the IP addresses associated with these URLs.

As we have discussed with you and your colleagues on numerous occasions, it is not technically feasible for WorldCom to block access to a site based on its URL if that site is not hosted on our network. Rather, the only technically feasible solution for WorldCom to block access to such a site is by means of "null routing" the IP address of the site, i.e., to instruct the routers in our Internet network to discard all IP packets destined for that IP address.

All devices on the Internet communicate with one another using IP addresses, which are typically represented as a series of four decimal values separated by dots (e.g., the IP address of the computer that hosts the Web site www.worldcom.com is 204.176.69.71). Because IP addresses are difficult for people to remember, Web browsers are designed to search for sites on the Internet using URLs, which are usually brief phrases that refer to an Internet server and its contents. A URL is actually made up of several parts. Take, for example, <http://www.worldcom.com/US/PRODUCTS>. "Http:" indicates that the HTTP protocol should be used for communication. "://www.worldcom.com" indicates that the information is at the Web site associated with the domain name www.worldcom.com.

"/US/PRODUCTS" indicates that within the Web site at the www.worldcom.com domain name, the information is found in the part of the Web server's filing system called "PRODUCTS," within the file directory called "US."

When a user types a URL into a Web browser, the browser uses the Domain Name System ("DNS"), which is like a group of phone books for the Internet, to look up the domain name part of the URL to match it with an IP address. The Domain Name System is a highly distributed and replicated hierarchical system that is not under the control of any one ISP. Indeed, the domain names found in the URLs listed in the Order are not actually translated into IP addresses by WorldCom's own Domain Name Servers. Rather, the servers that perform this translation are under the control of others. Thus, it is not technically feasible to block access to these URLs using the Domain Name System, as your office has suggested. Even if it were technically feasible to remove a domain name from WorldCom's DNS servers, this solution would not block users' access to the URL at issue, just as crossing a name out of a phone book would not prevent people from calling that phone number. Users could simply use a different "phone book" (i.e., DNS resolver) or "call" the number directly by using the IP address instead of the domain name.

In order to comply with the Order therefore, WorldCom must associate each URL with an IP address and "null route" that IP address. It is important to recognize that an IP address itself is not content; rather, it is merely a locator for content. A single IP address is analogous to the street address of an office building. Hundreds or thousands of completely unrelated businesses can have offices in the same building and share the same street address. Likewise, an IP address can be the "street address" of hundreds or thousands of different sites that are completely unrelated in content and ownership. For example, Terra.es, the hosting provider for one of the sites in the Order, is the largest ISP in Spain and one of the most popular portal sites in the world for Spanish speakers, including those in the United States. The URL listed in the Order appears to share an IP address with thousands of unrelated sites behind the Terra.es domain name. (Terra disabled the URL in question immediately upon being notified of its existence. It was able to do this because it controls the computers that host all of the users of the Terra.es domain name.) Only the service provider hosting the content (analogous to the landlord of the office building) has control over the specific sites behind the IP address. If an ISP such as WorldCom, which is not hosting the sites in question, is ordered to block access to a site hosted by another ISP, the result is to block access to the entire "building" and all the "businesses" located in it, i.e., to all the content associated with the IP address.

WorldCom will periodically check the IP addresses associated with <http://www.teen-teen.biz> and <http://love.xloli.com/?lustv.xloli.com> and, in the event the operator of one of these sites associates the domain name contained in the URL with a new IP address, we will update our systems to block access to the new IP address and remove the block on the prior IP address. In such case, there could be a brief period of time during which these URLs are accessible through the WorldCom network while we update our systems to block the new IP address, but the URL would again become inaccessible over the WorldCom North American Internet network immediately after the update is completed.

As we also have discussed with you and your colleagues, it is not technically feasible for WorldCom to block access to a site on the Internet only to subscribers located in the Commonwealth of Pennsylvania. Internet networks do not recognize the geographic boundaries of states. Moreover, users located in Pennsylvania can access the Internet through WorldCom's network by dialing toll-free numbers that terminate outside of Pennsylvania, by dialing Internet connection points in other states, and by using dedicated connections to the Internet that terminate in facilities in other states. As a result, there is no technically feasible way for WorldCom to comply with an order to block access to sites on other ISPs' networks without blocking access to these sites by all users of WorldCom's North American Internet network.

In sum, the inevitable result of WorldCom's compliance with the Order is to block access by all users of the WorldCom North American Internet network to all content located at the IP addresses

John J. Burfete, Jr.
September 23, 2002
Page 4

associated with the two remaining URLs referenced above, including but not limited to the specific items that you have identified as child pornography. I should point out that the actions by WorldCom described above will not result in the removal of the content in question from the Internet, nor will they necessarily prevent users in Pennsylvania and elsewhere from accessing the sites through other Internet Service Providers. We do, however, believe that we have done all that WorldCom can do to comply with the Order and to block access to the sites associated with the URLs listed.

Finally, I would like to reiterate that WorldCom has made repeated offers and efforts since 18 Pa.C.S. §7330 became law to work cooperatively with the Office of the Attorney General to devise solutions to combat child pornography in ways that do not adversely impact unrelated, legal content on the Internet. WorldCom shares your abhorrence of child pornography, and we are proud of our extensive efforts in cooperation with law enforcement agencies all over the world that are investigating and prosecuting those responsible for these heinous crimes. We believe that law enforcement and ISPs can most effectively and efficiently combat child pornography by identifying the service provider that has the ability to remove the content in question at its source and by cooperating pursuant to proper legal processes to gather evidence to bring to justice those responsible for creating and using such illegal content.

Sincerely



Craig Silliman
Director, Technology & Network Legal
WorldCom

cc: The Honorable Lawrence A. Brown