

Additional comments in Dockets 07-52 and 08-7 (filed in both dockets per Commission-established multiple-docket rules).

I have run across some additional information regarding some network management practices, this time regarding email, which I include for the record. This was found on Comcast's website, but I don't know where, as this was in a discussion board.

"When I went to the Comcast website to view their Policy18628, it said:

Mail to Comcast is rejected and is returned with an error message containing the code BL004. What does this mean?

Our filters have determined that email from your mail server has been sent in patterns which are characteristic of spam. In an effort to protect subscribers, your mail server has been blocked from sending email to the Comcast network. Mail servers are typically shared by many users so it may be the case that another party using your mail server has sent spam, even if you have not.

How do I get my IP removed from the blacklist?

It is important that your email administrator is aware of their outbound spam problem to avoid being blocked by Comcast in the future. When contacting your email administrator, you should include the error message contained in the email which alerted you to this problem. This error message contains important information to help your email administrator resolve this issue. Removal requests can be sent to www.comcastsupport.com/rbl and will require the IP address of the blocked mail server. Requests submitted through this form are monitored 24 hours a day, 7 days a week to ensure a timely response."

The above indicates that there are spam issues that some legitimate senders have, where they do not have implemented what is called a 'Sender Policy Framework' record, or 'SPF Record'. This policy is poorly worded, especially as it does not mention the 'SPF Record', and it should focus on how to resolve the issue rather than saying, 'that's it, you're skunked'.

They (Comcast) are using what is known as the 'Realtime Blackhole List', which is good but at times has had a checkered past. See the anti-spam forums on Usenet/Google Groups and elsewhere for discussions on what this is and how this list is supposed to work or not work.

ISPs need to be required to disclose the types of end-user tools that can be used to better manage their traffic, prevent spam (reported to be as much 90 percent of all email sent at times), and other types of network management practices on the site's end. The ISP needs to be required to 'keep

their claws out of it' unless it is to stop a botnet or for other legitimate reasons related to illegal activity as I have discussed before. By disclosing the types of tools the end user (web site and email admins) can use, they can allow end users (site/mail admins) resolve a good number of these, leaving the trickier ones to be tackled, thus reducing costs to both the end user and the ISP. This would comply with the Regulatory Flexibility Act if it were implemented.