Robert M. Topolski
6815 NE Vinings Way Apt 922
Hillsboro, Oregon 97124
(503) 342-2468

April 3, 2008

David Cohen
Comcast Corporation
One Comcast Center
Philadelphia, PA 19103-2838

RE: your letter addressed to FCC Chairman Martin, dated March 28, 2008
http://fjallfoss.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6519869393

Dear Mr. Cohen:

I am a Comcast customer. I have continuously had Internet service with your company since it became available in my area several years ago. I first noticed something wrong with the service during the winter of 2006-2007. When I finally narrowed it down to Comcast's intentional interference, I posted about it on a forum popular with technical enthusiasts.[1]

This is in response to comments in your your FCC EACS filing
http://fjallfoss.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6519869393
which is a letter addressed to FCC Chairman Martin, dated March 28, 2008, regarding your disappointment with his comments following the BitTorrent/Comcast announcement. You said,

> **David L. Cohen said:** In your statement yesterday, you continued to repeat the unsupported and inaccurate assertion by some critics that Comcast "arbitrarily block[s] certain applications on its network."
>
> As we have unambiguously stated on the record, Comcast's customers have been, are, and will continue to be free to access any lawful Internet content and to use any application and service of their choice, including those that utilize peer-to-peer ("P2P") protocols. As we have explained in detail, Comcast engages in minimally intrusive, reasonable network management practices that occasionally delay some unidirectional P2P uploads (not downloads, and not uploads that occur while a download is in progress) only when necessary to prevent network congestion. These practices do not deny our customers' access to these applications and services, but rather and enable the use of these and countless other applications and services by ***all*** of our customers.

[1] TI - Comcast is using Sandvine to manage P2P Connections - dslreports.com - 2007-05-12
UR - http://www.dslreports.com/forum/r18323368-Comcast-is-using-Sandvine-to-manage-P2P-Connections

I wish to help you as well as everyone else accurately understand these issues ahead of the upcoming meeting at Stanford. You (Mr. Cohen) are not a technologist and you can only report what you've been told. I, however, am professionally qualified to run these tests and report the results accurately. As a technology professional, my reputation is on the line. Since this letter is meant for wider readership than the addressee, please forgive me for slipping in and out of first-person and third-person grammar. Likewise, my observations are limited to those possible from my own Comcast connection in Hillsboro, Oregon. One might easily assume, however, that Comcast attempts to enjoy the economy of scale possible when outfitting its numerous head-ends, and aggregation points with similar equipment configurations.

My bio is file with the Free Press's original filings in this matter. In short, I'm a recognized testing and networking professional with experience spanning over 25 years. In 2004, I earned my qualification as a Certified Software Quality Engineer by the American Society for Quality. In 2006, I was awarded the Most Valued Professional status in the Networking area by Microsoft. Indeed, my professional career in Software Validation and Quality Assurance is weighted heavily in networking.

I am not a peer-to-peer enthusiast. I am, however, a music and history enthusiast. I enjoy tunes from the Tin-Pan Alley days, 1890-1910. While attempting to share some copyright-expired items I had converted into digital format, I found that Comcast continuously interrupted all of those upload attempts by injecting forged RST packets into the TCP conversation.

These RST packets were forged so that they would appear to come from an end-point's IP address with the correct sequence number values. By doing so, these packets successfully bypass a feature of the TCP protocol which prevents acting on packets with invalid sequence numbers.[2]

> **David L. Cohen said:** unsupported and inaccurate assertion by some critics that Comcast "arbitrarily block[s] certain applications on its network."

Comcast's behavior is accurately described as both arbitrary and blocking.

By blocking, I mean that successfully established and working TCP connections were torn down by an unexpected RST packet. Normally, TCP connections are ended using a FIN sequence.

By arbitrary, I mean the classic dictionary definition of the word, arbitrary[3].

---

[2] TI - RFC 793 - Transmission Control Protocol
UR - http://tools.ietf.org/html/rfc793#page-37
In all states except SYN-SENT, all reset (RST) segments are validated by checking their SEQ-fields. A reset is valid if its sequence number is in the window.

[3] TI - arbitrary - Definition from the Merriam-Webster Online Dictionary
UR - http://www.merriam-webster.com/dictionary/arbitrary *(continued on next page)*

> **David L. Cohen said: "**[arbitrarily block(s)] certain applications on its network."

It is truly impossible for Comcast to prevent a user from launching a client program, also known as an application. However, if such an application is an Internet application, Comcast can render such a program useless by identifying and blocking the network communications of that program.

Comcast blocks certain functions of P2P applications, specifically the upload function.

When tested, the Gnutella P2P protocol was blocked from uploading 100% of the time from mid-winter 2006-2007 until late February 2008.[4] The ED2K P2P protocol was blocked from successfully uploading approximately 75% of the upload connections. The BitTorrent P2P protocol was blocked on about approximately 40% of the connections. These percentages remained consistent regardless of the time tested or the day of the week.

Technical Note: In the text that follows, I describe certain attempts at using a protocol for uploading as nn% blocked. The percentage is determined by the number of RST-ended connections divided by total current and ended TCP connections. These tests were conducted using content that I was authorized to distribute. Some examples include recently released versions of Ubuntu or Knoppix Linux, OpenOffice, a text version of Leonardo DiVinci's notebook, and digitized versions of music obtained from wax cylinder disks. When available, protocol obfuscation features such as encryption, padding, and delayed bitfield handshakes were disabled. For BitTorrent, a single file was being offered. For ED2K or Gnutella, multiple files of the nature described above were being offered. Measuring begins after the first 10 minutes and ends when a plateau is reached in the results. A balance of 33% to 67% seeders (strictly uploaders) and downloaders is sought as a file too heavily or lightly available will skew the results. Results attributed to Comcast's interference should be compared against a background of RST-caused disconnections of approximately 3% to 8% (the amount of interference caused by normal failures and interference by the ISPs of the remote peer or the intermediate transit providers). With ED2K, the "Total failed upload sessions" information on eMule's statistics page is used instead of the RST/Connections calculation. Given this information, these tests and results should be reproducible by anyone.

(continued from previous page) 1**:** depending on individual discretion (as of a judge) and not fixed by law <the manner of punishment is *arbitrary*>2 a**:** not restrained or limited in the exercise of power **:** ruling by absolute authority <an *arbitrary* government> b**:** marked by or resulting from the unrestrained and often tyrannical exercise of power <protection from *arbitrary* arrest and detention>3 a**:** based on or determined by individual preference or convenience rather than by necessity or the intrinsic nature of something <an *arbitrary* standard> <take any *arbitrary* positive number> <*arbitrary* division of historical studies into watertight compartments — A. J. Toynbee> b**:** existing or coming about seemingly at random or by chance or as a capricious and unreasonable act of will <when a task is not seen in a meaningful context it is experienced as being *arbitrary* — Nehemiah Jordan>

[4] TI - Comcast is using Sandvine to manage P2P Connections - dslreports.com
UR - http://www.dslreports.com/forum/r18323368-Comcast-is-using-Sandvine-to-manage-P2P-Connections

In late February, both EFF's Peter Eckersley[5] and I noticed[6] a dramatic change in what had been, to that point, very consistent results. As of February 20th, interference with Gnutella and ED2K had stopped. Interference with BitTorrent has increased to 75%. Subsequent tests have maintained those new values.

> **David L. Cohen said:** Comcast's customers have been, are, and will continue to be free

The word "free," as used here, implies no encumbrances or "delays" or blocking. Clearly, "free" is simply an inaccurate characterization. More accurately, "free" can only mean that customers are "invited to try."

> **David L. Cohen said:** to access

Since a distinction is frequently being made about "accessing," "uploading," and "downloading," it needs to be noted that Comcast's installation of Sandvine is at the metropolitan area's aggregation point[7], and thus affected Comcast peers trying to download from Comcast peers. Therefore, if "accessing" only means "downloading," the statement is still falsified as a Comcast customer's download is interrupted if the uploader is also a Comcast customer[8].

> **David L. Cohen said:** any lawful Internet content

There currently is no known technology available[9] to accurately discern between "lawful" and "unlawful" content. Also, the Sandvine technology employed by Comcast does not purport to discriminate between lawful and unlawful content. The blocking, therefore is performed on both lawful and unlawful content.

Furthermore, my motivation for starting this investigation was that I could not upload the public-domain musical content -- all attempts were blocked around-the-clock. The OpenOffice (Open Source) suite I attempted to upload to the EFF was blocked. The Holy Bible (Public Domain) was blocked.

---

[5] TI - [NNSquad] Comcast interference subsides?
UR - http://www.nnsquad.org/archives/nnsquad/msg00541.html

[6] TI - Re: Comcast is using Sandvine to manage P2P Connections - dslreports.com
UR - http://www.dslreports.com/forum/r20055371-Changes_In_Behavior

[7] http://www.dslreports.com/forum/r18936691-SandvineBoxFound

[8] http://www.dslreports.com/forum/r18918622-Comcast2Comcast

[9] TI - Internet Evolution - The Big Report - Peer-to-Peer Filters: Ready for Internet Prime Time?
UR - http://www.internetevolution.com/document.asp?doc_id=148803&page_number=1

David L. Cohen said: and to use any application and service of their choice, including those that utilize peer-to-peer ("P2P") protocols.

If a Comcast user chooses a Client-Server application to transfer files, such as a web-browser client or an FTP client, the sessions are allowed unmolested.

However, if a Comcast user chooses a Peer-to-Peer application, such as uTorrent or Vuze, the communications by that application are eventually met with Comcast's forged-injected RST interference as it tries to upload to a peer who is not simultaneously downloading.

It should be also be noted that Comcast customers use of "servers" for file-sharing is very restricted by their Acceptable Use Policy[10]. While Comcast's AUP has never banned personal network Servers, it does ban establishing Public Services or Servers. The text of the section is obtuse enough that many members of the Comcast Forum on DSLReports believes that Comcast's AUP essentially says, "No Servers."[11]

Effectively, the only remaining file-transferring applications and services not receiving some kind of restriction are Clients performing transfers to/from Servers.

David L. Cohen said: Comcast engages in minimally intrusive

In order to do what Comcast is doing, it has to look beyond an ISP's traditional cues used for packet routing and prioritization (the IP header) and look at the payload inside of the IP packet[12] to determine how to handle delivery of the packet.

Apt analogies include a package delivery service opening a box to determine, based soley on their own judgment, if the item inside is disposable. Or, a letter carrier opening your outgoing mail to determine if the contents qualify for "junk mail" handling.

[10] TI - Comcast.net Terms Of Service - Acceptable Use Policy
UR - http://www.comcast.net/terms/use/#prohibited
- use or run dedicated, stand-alone equipment or servers from the Premises that provide network content or any other services to anyone outside of your Premises local area network ("Premises LAN"), also commonly referred to as public services or servers. Examples of prohibited equipment and servers include, but are not limited to, e-mail, Web hosting, file sharing, and proxy services and servers;
- use or run programs from the Premises that provide network content or any other services to anyone outside of your Premises LAN, except for personal and non-commercial residential use;

[11] http://tinyurl.com/55dxav

[12] http://en.wikipedia.org/wiki/Deep_packet_inspection

The phrase “minimally intrusive” suggests that there are few lesser intrusive options, and many more intrusive options. Simply untrue. For an ISP to do its job, there is no reason to look any further than the IP header, which contains the destination address and instructions on handling. IP was explicitly designed to facilitate a service provider's job. The payload beyond the IP's header is not the concern of an ISP. Except for Law Enforcement officials conducting authorized surveillance, the point beyond the IP packet header is only intended for the recipient. Anyone else looking at the payload usually wants to change the normal handling of the contents, change the content itself, or to collect information for future marketing.

There may be a "Reasonable Network Management" cause to do this, but it would be done reactively to investigate whether user-applied or application-applied priotization instructions in the IP header are being abused by a user to exploit prioritization as described in the Official Internet Standard Protocols. However, taking intrusive actions to prevent network abuse is traditionally done reactively -- either initiated by poor network performance or a complaint by other Internet users. An ISP inspecting payloads to apply its own sense of priority exceeds the definition of "minimally intrusive" and might also be considered to be something more than "Reasonable Network Management."

David L. Cohen said: reasonable network management practices

While I hold the opinion that there is nothing “Reasonable” going on here, the word used with “Network Management” has its history from the multitude of uses of the word "unreasonable" in the Carterphone decision.[13] The “reasonable person” being the common or consensus perspective of an average persons looking at a question of law, the word holds special weight when used in a court decision. Since my own point of view is steeped in the historical and technical histories of the Internet invention, my views probably do not qualify to sustain or refute the claim of reasonableness. Instead, I can only contribute to the facts and knowledge needed by a decider of fact to determine it.

I can, however, authoritatively state that my research has found no authoritative judgment of “reasonable” has ever been handed down by such a decider of fact in a case involving packet inspection resulting in protocol discrimination by injecting forged RST packets to tear down established communication links. In fact, my research finds law to support the position that the use of such technology by a Common Carrier violates The Communications Act SS 202(a), "It shall be unlawful for any common carrier to make any unjust or unreasonable discrimination in charges, practices, classifications, regulations, facilities, or services for or in connection with like communication service, directly or indirectly, by any means or device…". While Comcast is not a common carrier, this law sets applicable precedence and expectations by reasonable consumers who do not understand the difference (*this final sentence exceeds my technical evaluation and is purely my own opinion*).

[13] http://www.uiowa.edu/~cyberlaw/FCCOps/1968/13F2-420.html

David L. Cohen said: that occasionally (also "only when necessary to prevent network congestion.")

In all cases, and as mentioned before, blocking at about the aforementioned percentages was consistent 24 hours a day, every day of the week. When tested, the Gnutella P2P protocol was blocked from uploading 100% of the time from mid-winter 2006-2007 until late February 2008.[14] The ED2K P2P protocol was blocked from successfully uploading approximately 75% of the upload connections. The BitTorrent P2P protocol was blocked on about approximately 40% of the connections. These percentages remained consistent regardless of the time tested or the day of the week.

These tests have been conducted from May 2007 to present day.

While the results finally changed about February 20th[15] (perhaps owing to a software upgrade or a configuration change), the new percentages remain consistent 24 hours a day, every day of the week.

David L. Cohen said: delay

In so much as you can only delay a telephone conversation by hanging up on a very persistent caller, Comcast uses the same meaning of the word "delay" to describe its behavior here. However, it is not an apt metaphor.

With Gnutella, all uploads were always blocked 100% of the time, 24 hours a day, seven days a week. As I was offering a unique collection to members of that network, I was the sole source for those files. Therefore, those uploads weren't merely delayed, they were blocked since there were no other sources.

Similarly, the Holy Bible torrent created by the AP was a valid representation of a unique file (it would be given a unique "info hash," a calculated number that uniquely identifies the specific archive created by the AP. All unique BitTorrent archives have a unique info dictionary and would calculate to a unique key identifier. The AP aptly demonstrated that its attempt to upload the contents of its newly-created BitTorrent archive was not delayed, it was blocked.[16]

[14] TI - Comcast is using Sandvine to manage P2P Connections - dslreports.com
UR - http://www.dslreports.com/forum/r18323368-Comcast-is-using-Sandvine-to-manage-P2P-Connections

[15] TI - [NNSquad] Comcast interference subsides?
UR - http://www.nnsquad.org/archives/nnsquad/msg00541.html

[15] TI - Re: Comcast is using Sandvine to manage P2P Connections - dslreports.com
UR - http://www.dslreports.com/forum/r20055371-Changes_In_Behavior

[16] AP tests Comcast's file-sharing filter
http://www.usatoday.com/tech/products/2007-10-20-2072341885_x.htm

Across all of the protocols tested, blocking at the reported percentages was consistent 24 hours a day, every day of the week.

Comcast's use of the word delay can only be true when assuming that other members of the P2P network have the same files or parts of files. It is true, when a Comcast users is unable to upload a common piece of data to the swarm, a downloader can get it elsewhere. However, as the second largest ISP in the United States, Comcast users often find themselves with that unique piece of data necessary to complete an upload. In that case, the Comcast user must successfully upload his unique data before other users give up on ever completing the transfer.

David L. Cohen said: Some

After February 20th, interference to BitTorrent increased to the point where 75% of all established, unencrypted* connections were being terminated by RST. The remaining 25% of connections were to or from other uploaders, who disconnect in the normal way once it is determined that neither party wants nor needs any data. The net effect, however was that 75% interference level resulted in 100% of uploads being blocked on BitTorrent.

(*The use of encryption to obfuscate the BitTorrent protocol does help improve this number by about 25%, which is a reason why some report a lower level of interference or a higher degree of success.)

David L. Cohen said: unidirectional P2P uploads (not downloads, and not uploads that occur while a download is in progress)

The Sandvine device interrupts unidirectional TCP connections, but it is inaccurate to say that it does not interrupt while downloading. While downloading, some flows are unidirectional simply due to a moment in the normal BitTorrent rhythm of choking and unchoking (which prevents several peers from transferring data across the link at the same time). Other flows are unidirectional because the Comcast peer already has all of the pieces held by other peer. Because of these behaviors, Sandvine will interrupt connections between two "downloading" peers.

Sandvine does not detect "BitTorrent Upload" swarms (connections between the Comcast customer and multiple peers involved in transferring parts of the same file). Instead, Sandvine inspects packets in individual connections. Therefore, it cannot know whether a particular user is attempting to seed (upload only) or receive (both uploading and downloading) a file. Instead, it can only determine the activity of the protocol within the limited window that it monitors. Therefore, it can make the mistake of marking a connection as "allowed" if it starts bidirectionally, even if it later switches to unidirectional[17]. It likely also makes the mistake of blocking a connection that is a downloading (bi-directional), but is waiting its turn to make a request from the remote peer.

> **David L. Cohen said:** only when necessary to prevent network congestion.

See "occasionally," refuted above.

> **David L. Cohen said:** These practices do not deny our customers' access to these applications and services,

See "delay," refuted above.

> **David L. Cohen said:** but rather and enable the use of these and countless other applications and services by all of our customers.

In as much as the interference is constant around-the-clock, it is not clear to me that it does anything but block certain key features of certain applications by customers.

Furthermore, Comcast already has bandwidth limits in place that divide its substantive bandwidth between its customers. Nothing that I can do with a P2P client will allow me to exceed the limits that I have purchased and that Comcast programs into my cable modem.

Therefore, Mr. Cohen is making a technical claim that can only be the case if the Comcast customers who are sharing bandwidth are regularly exceeding the bandwidth available. As Comcast divides its bandwidth by selling portions (tiers) with modem-enforced limits, it appears that Comcast may have failed to predict and keep ahead of customer demand. As a result, customers are not finding the bandwidth described by Comcast when they purchased the service.

Yet, the idea that Comcast cannot meet bandwidth demand is falsifiable. Comcast CTO stated in May 2007, "For one, we're splitting a lot of nodes based on the success of voice,

[17] UR - http://www.dslreports.com/forum/r19998772-Sandvine_achilles_heel

high-speed Internet, and VOD. In other words, all based on downstream requirements, not upstream.

"On HSD (high-speed data), I'm using two to three 3.2 MHz carriers (upstream). A lot more than that are sitting fallow in my CMTS cards. In most markets, I still have 12 MHz of bandwidth I can reclaim from circuit switched voice, once we migrate off of those platforms. So for now, the 5-42 MHz to me seems plenty adequate."

Werner continues to describe that most bandwidth crunches are anticipated, and inexpensively satisfied, " I have started looking at node splitting here. The nice thing about node splitting is, it works so well, from an efficiency perspective. Say you have a market with 30 percent penetration of HSD. Some neighborhoods might have 15 percent penetration, while other real hot spots might have 60, 70, 80 percent. There, we may split to 125 homes.

"But it's all usage driven. As we hit 70 percent utilization, we issue a work order to split the node. But it depends on utilization. Usually we set it to split to 250 homes. And for us, 65 percent of our node splits are really decoupling of nodes at the headend. Maybe you had three or four nodes sharing a laser. We call that a virtual node split."[18]

IN CONCLUSION, Comcast's continuing characterizations – which you have consolidated in your letter – are both technically incorrect and effectively obfuscate the details of the actual behavior of Comcast's network. The characterizations, both in part and has a whole, are false. In so much as you can only report what you have been told by technologists, you may not have been aware of the actual details. Now, you are. And if you do not believe me, you are at least morally obligated to get independent verification of these truths. Because, at a minimum, I am a customer and I have an unresolved technical support problem.[19]

Respectfully,

/s/
Robert M. Topolski

cc: Sent via email, posted to DSLReports, and filed in FCC EACS.

[18] http://www.cedmagazine.com/how-sexy-is-hfc-answer-plenty.aspx
How Sexy is HFC? (Answer: Plenty.)
Compiled by Leslie Ellis, Independent Technology Analyst
CedMagazine.com - May 01, 2007

[19] http://www.dslreports.com/forum/r18901363-NoTechnicalSupport