

**Before the
Federal Communications Commission
WASHINGTON, D.C. 20554**

In the matter of

Framework for Broadband Internet Service

GN Docket No. 10-127

COMMENT

I like trains. Especially those steam engines of long ago. For me its just a hobby. I suppose some 150 years ago, there was some real interest and concerns over an important nation building transportation system. Farmers wanted to get goods to market cheaply, and Train companies wanted to maximize profits – what we all know as the “what the market will bare” policy. Looking solely at court records is a poor choice of reviewing history. History that seems all to be able to repeat itself.

Today we have 29 percent (or was it unlimited, I forget as it changes all too often) interest rates. Whimsical banking fee's. There was a 60 billion dollar ponzi scheme. How about Enron. The housing market securities meltdown. Microsoft monopolistic business practices. Did I forget the big oil spill by the gulf states?

Some 10 years ago, around 2000, I did not perceive any of the issues that are now before the commission. 10 years ago my main issue was obtaining internet access locally via the Plain Old Telephone System (POTS) for just the cost of a phone call. The services provided by the ISP's then had to provided by those entities, as those providers of internet service are always on, and connected to the internet¹. To encourage usage, they provided e-mail service, local DNS service, maybe some non-commercial web service, access to News Groups.

Some 10 years one could buy a T1 (1440Kbps) dedicated internet connection for about one thousand dollars a month. Not exactly an incentive to get 'always on' and connected internet service for a residence. Even with that T1 connection, one does not automatically get DNS, MAIL, WEB, NewsGroup service as part of the T1 connection. You have to buy your own facilities, your own computer, your own programs , and provide your own administrative talent.

10 years ago Internet port blocking did not exist². Internet speed throttling was accomplished naturally, just like the reduced throughput on the 5 lane Los Angeles highway 5 at the 5 o'clock rush hour. And broken connections (I'd like to believe) was because of electrical noise, rather than than the ISP's deliberate attempt to actively manage usage.

10 years ago, in my opinion, the internet as was practiced then, was OK.³

- 1 Email processing and storage services was done locally at the ISP's site. For e-mail service to directly reach residences would mean that the residential computer would have to be mostly on and connected to work reliably. News Groups is a system where a lot of group topics are centrally located and access. To fully participate, and ISP needs a fairly spacious internet connection, so news group access may have been farmed out to another ISP. A 56kbit residential modem just would not keep up with the amount of submitted news group information.
- 2 Even though internet port blocking wasn't practiced, it was possible. Not further down the road, Verizon opted to block residential incoming port 80 access. The premise was to prevent, at that time, a virus (or) from overburdening the network. That was over 9 years ago. A complaint to the FTC, and then passed on to the FCC resulted in no action.
- 3 It is OK because I was able to have internet access in mostly urban areas. Is is OK because one could overcome, with

A lot has happened in those 10 years. A really neat POTS wireless system, for those who are willing to pay some \$300 per year. How about that triple play (telephone, television, and internet) program for \$1200 a year. And Verizons similar offering for \$1000 a year. Did I mention I got a 1.4Mbps 'always on' DSL connection for \$39 a month from Verizon. I no longer have to monopolize the phone line, or get a second phone line.

Today I have a DSL connection at 3Mbps for \$32. It was nice that Verizon also offered e-mail and NewsGroup services as part of the offering, but I only needed access to the internet. It did not matter if the ISP was a facility only service, or one that actually owned the transmission facility. They both provided the same Internet Access , from the residence to the internet.

To Start Off, some Corrections.

DNS⁴ miss classification as a connection service, rather than an information service.

DNS is, simply put, a means at which names are associated with IP addresses, as well as the reversal. The resulting numeric IP address is then fed into the internet connection services 'dialing' mechanisms.

DNS is akin to telephone 'Operator' services. If you dont know the number of the entity you want to call, you can ask for that number from that service. If the number was at all publicly available, then the operator will tell you that number. At one time, the 'Operator' would also dial it for you. Telephone subscribers would have their names, addresses, and a static phone number published in the 'white' pages phone book. Commercial entities would have to pay to enter their name, business, and phone number entered into a 'yellow' pages phone book.

DNS is more like the internet version of the 'yellow' pages. If you wanted to be known by a unique name through out the world, then you pay a Domain Registrar (which may be your own ISP) to have your name entered in the DNS information system.

There is no DNS 'white' pages. Residential customers, are not automatically listed into the DNS system. And neither are commercial customers. Customers has to do that themselves.

Your local ISP does not even have to provide DNS services. Anyone needing to use DNS services only has to locate the top level registrar 'well published' IP numeric addresses to locate the computer/registrar that has the name and its associated numerical IP address that you are looking for.

Why do ISP's even bother with DNS? Well it has something to do with internet traffic bandwidth. If an ISP does not provide for DNS services locally, then those DNS informational requests would go outside their system, and further increase the usage of limited internet bandwidth. Successful matches of names and numbers can then be remembered locally, and be answered quickly . Only unknown names would be sent outside for an answer to what the numerical IP address would be.

Can you use someones elses' DNS services? Yes you can. It was typically bad form to use another ISP DNS services. It used up your ISP's bandwidth, and it used the bandwidth of the other ISP's. But you may get a reliable DNS service in return , as your local ISP may administratively suck at it. Many ISP's now block outside access to their own DNS services. You can now buy DNS services from other providers. This was usually done as a backup in case your ISP's computer went offline for one reason or another.

Can the Internet connection service work with out it? The answer would be yes. Its as much as one would ask "Can the Telephone system work without the 'Operator'" service that has been so much a part of the phone system. I think it can. Its a bit more work, as one would have to use a phone book, or

some internet trickery, the Verizon permanent blocking of incoming port 80 for residential customers.

4 Domain Name Service

use the postal system to request the numbers of friends, relatives, and commercial enterprises. There will always be a dial tone. But you will still need a number to dial.

Many other Informational program services require the informational services provide by DNS in order to translate a text name to a number. A lot of those informational services also accept numbers in addition to names. Without it, humans would have to remember thousands of numbers to thousands of internet places.

BTW: ISP's have altered the way in which failed DNS lookups are handled. When a user provides a non-existent domain name, instead of an error, the ISP provides a web page with commercial advertisement. Verizon is not the only one that does this. I have been informed that Embarq also does this.

Indistinguishable Internet Offering

Its hard for me to differentiate a provider of ISP services and that of directly connecting to the internet. Even if I dial using a telephone and modem to connect to the ISP, the service provider would have to allow me to connect directly to the internet. If the service only want to provide information, and no internet access, then those shops have been traditionally called computer shops with dial-up access.

Even if the only thing offered by the ISP is an internet connectivity service, meaning that the information from my site reaches the internet (dial-up, broadband, satellite, wireless,) then that entity is an Internet Service Provider. Once that connectivity service is withdrawn, that business fails to be an Internet Service Provider.

A hotels main business is to offer rooms. As part of the hotels charm, it offers many amenities. Pool, cable TV, continental breakfasts, security, parking, air conditioning, internet access, telephone access, exercise rooms, and so on. For the hotel provider, such amenities induce clients to stay there, rather than to somewhere else less accommodating. A hotel, as every one knows, will provide at the very least a room. A Hilton hotel, will also provide for a room, as well as many amenities, recognized as part of the Hilton business style.

An Internet business is not an ISP if it does not, at the very least provide for “internet connectivity” to its clients. Amenities like e-mail, newsgroups, web storage⁵ are all enticements to sign on with this ISP. If you do not utilize their amenities, then one can look at Google for e-mail services. One can look for other businesses that offer web services in competition to your ISP.

But without that fundamental connection service, you cannot gain access to competing informational services.

No One Offers separate Telecommunications Service

I found it interesting that the FCC would suggest that many of the “providers – including more than 840 incumbent local telephone companies – currently offer broadband transmission as a telecommunications service expressly separate from their internet information service.”⁶

I have looked. I found none that would provide me with simple broadband connectivity service for the same price as what I pay for with a service that had informational services. Maybe they have the service, but don't market, or advertise its availability.

⁵ Web storage is somewhat useless, as most ISP's wont create domain name entries pointing to the users simple web pages.

⁶ Paragraph 21 FCC 10-114

Some ISP's appear to want to sell you this offering, but at a price that is some 2 to 8 times (\$60 to \$200 per month) than I now pay (\$32 per month) for.

I suspect that the FCC would be rather surprised if they actually did some research.

Managed or Specialized Services

Internet is not designed to be a Real Time service.⁷

The plain old phone system (POTS) is an example of a (almost) real-time communications system. Delays in the plain old phone system is just not acceptable to the human ear.

Internet phone calls, or VoIP, have this same issue. Delays in sending or receiving the VoIP data also cause issues with humans.

Video services do not need to be broadcast in real time. Buffering of 10 minutes of video data may be accomplished in just 1 minute. Adequate broadband throughput can be used to fill in the 10 minute buffer to smooth out the inherent delays in reception of video data. Maybe a TiVO approach would be a better than granting specialized service status to any ad-hoc service a business or service may want.

Internet as Telecommunications Service

It quite clear from the results of the Comcast Court case, and some of the suggestions by the various incumbents, that the fox's still manage the roost. For some 20 or so years, the fox, and the chickens lived in a fairly harmoniously fashion. One day, one of the foxes was caught in the act of disturbing the chickens. A disturbance not based on random acts of god, but rather a deliberate attempt to alter the environment to the detriment of the occupants.

Now the FCC has the task of re-determining how much they should trust the current business methods that the fox has. After all, its in the fox's nature to do whats best for the fox. So in the 10 years that I am familiar, I suppose the writing on the wall is that the ISP's have found an internet business model potentially more profitable than just providing connectivity services.

I suppose it now appears that the FCC is in the process of classifying the parts of the internet as a regulated utility, and the other parts that use the utility to transport information from one place to another.

Telecommunications Service as a Fundamental ISP Component

When I buy Internet access from an ISP, I expect at the very least, direct access to the Telecommunications connectivity component. With that direct access, I can connect to any other numeric IP address on the Internet of my own choosing.

If I wanted to connect to a particular registered domain, then I can use either the domain services offered by the incumbent ISP, use my own, borrow from another ISP, or purchase DNS access.

If I dont like the Web Browser offered by the incumbent ISP, or the browser offered by the Windows Operating system⁸, I can obtain the Netscape browser, or the Google browser, or Mozilla.

⁷ Paragraph 108 FCC 10-114

⁸ A notable court case between Microsoft and Netscape. Because Microsoft was the owner of the Operating System that so many customers use, Microsoft had a overwhelming advantage in bundling its browser with the cost of the OS. Other providers of browser software had very little chance in competing at this level.

If I don't like the e-mail service offered by the incumbent ISP⁹, I can build my own, purchase another service, or use a free service.

And if the ISP no longer offers News Group information service, I could buy into another service¹⁰, build my own¹¹, or stop using that type of information service¹².

All these things I can do, and still retain the ISP as an internet connection provider. I can overcome those short comings, because I have control over my computer. I can buy informational services from anyone in the world, so long as I have the capability of connecting to that internet end-point.

BUT once the data leaves my premises, I have absolutely no control as to how the data is transmitted to the end-point. I cannot suggest satellite, nor fiber optics, nor the shortest path to the destination. Nor do I want to, as this interferes with the (best?) efforts of the communications provider to provide competitive service.¹³ Comcast now demonstrates that ISP's may not have those internet customers best interests at hand. The promises once made long ago, are no longer a hallmark for the provider of those connectivity services.

It is clear from the Comcast case, that Comcast was concerned with a information transfer program. It is clear from third party testing, that the interference in the connectivity service(s) was the means at which to accomplish their goals. Its just not clear to the ultimate purpose. Did Comcast want to poison the reputation of the bitTorrent scheme? Did they want more bandwidth allocated to their new video services? I guess we will never know for sure as to why. All we know for sure is that they did.

What of other ISP's interference with connection services? Verizon has, for some 9 years blocked incoming connections to port 80 (Web Services) . A formal complaint to the FTC, and the FCC provided no relief. This action is not advertised by Verizon. The reason for the deliberate interference is long gone. Yet the interference is still being done.

Late 2009, Verizon has terminated my ability to send e-mail from my own home e-mail service. Promises made by Verizon in 2005 to the FCC was made in bad faith, as they blocked internet port 80 before the promise, during the promise, and after the promise. Now that Verizon is blocking my outgoing e-mail, it just another feature of the Verizon connectivity service that has been turned off. There was no appeals. No offer to mediate my concerns. No compensation for the loss, or for the costs at obtaining an alternate service.

9 Verizon was (class actioned) sued for destroying legitimate email. Verizon, without notice, changed its e-mail policies to refuse e-mail from places Verizon did not like. Verizon has since changed its (unknown) blacklisting policies.

Unfortunately, those policies still blacklist many legitimate sources of e-mail. E-mail from my domain is still blacklisted by Verizon, even after several requests for removal.

10 There are many organizations that offer New Service, circa the year 2000. Since Verizon had such an offering as part of their information services, I used it.

11 Building your own, although feasible, requires a lot of bandwidth 24 hours a day, 365 days of the year.

12 This is the case when Verizon stopped offering News Group access. For many years, Verizon owned, and managed their own News Group System. The New York State Attorney General Cuomo and Verizon agreed to stop Child Pornography on the News Groups system that Verizon managed. Out of that agreement Verizon eliminated some 10,000 legitimate discussion groups. Verizon did not eliminate all news groups, but substituted some benign, uninteresting discussion groups. Soon thereafter, Verizon eliminated the news group offering all together – lack of interest it was suggested. Writing to NY Senator Schumer did not elicit any reply. Verizon offered no substitute service. Verizon offered no reduction in pricing.

13 In the year 2000, no one would have thought that the service connection between 2 internet points would be diminished in any fashion. It was presumed that the ISP's would provide their best efforts into reliable and speedy data transmission. With Comcast, we see that those perceived goals that consumers want, and have paid for, are not necessarily what the commercial internet service providers are willing to provide anymore. Even if there is no evidence that consumers are harming the network.

Verizon chose to block only a class of internet consumers. It did not block those services to commercial outfits. It did not block those services to itself.

Nor was the FCC of any help in this issue. My complaint of Nov 2009, was made before the Comcast decision. My complaint was responded to by Verizon¹⁴. My follow up replies to the FCC regarding Verizon's response went unanswered¹⁵. When I inquired about the complaint, I was informed that the complaint was resolved¹⁶, with no response or comment from the FCC. I now have to wonder if the rights of the internet consumer as expressed by the chairman, and commissioners had any meaning before the Comcast court decision. In my mind, it was clear that what Verizon has done was a violation of the service connectivity commitment, and principles as expressed by the FCC.

In Summary, it seems that the current method of protecting the customers legitimate usage of connectivity services appears to be flawed. Flawed in that any provider of connectivity services can simply disrupt the legitimate usage of those connectivity services. Whether or not there is a factual basis for the ISP's concern, appears to be irrelevant. There is no appeal from the ISP's business model. Then there is the addressing of complaints to the FCC. There does not appear to be any form of appeal from which the complainant believes is resolved contrary to current FCC position.

The only stable solution to prevent further connectivity degradation, and FCC complaint resolution is to classify the connectivity services (less the DNS information service) as a protected service, that does not discriminate on any basis¹⁷. The closest equivalent would be the Plain Old Phone System – from the wall jack to the central switching offices. There most have been some regulation that prevented the phone company from disallowing FAX machine, Acoustic modems, and the various phones that can be connected to the POTS. No one is suggesting to the POTS provider on how to manage the connectivity issues, but it becomes irrational for the POTS to deny FAX service to residential customers, and allow that service to used by commercial entities.

Other Approaches to Oversight

Yes, we seem to be in some agreement that some policing is in order. Its also important for national security. Yet I am rather reluctant to have technical oversight given to purely commercial interests. For instance, the issue of spam¹⁸ is being addressed by a consortium call MWAAG¹⁹. One of MWAAG's suggestive spam remedies is to block all access to the standardized e-mail internet port to all residential customers, irrespective of any wrong doing by the customer²⁰.

Verizons undisclosed spam preventative policy has led to a class action suit for failing to disclose, and for failing to deliver legitimate e-mail²¹.

And then there is Verizons approach to blacklisting through various Spam prevention systems²². Here Verizon is informing the world that the IP numbers used by its customers should not be sending e-

14 Exhibit C

15 Exhibit D

16 Exhibit A. Exhibit B

17 Specialized services, such as internet telephone, or Video Feeds should **NOT** be granted any favored connectivity status. Should someone who is paying for "Tripple" services (telephone, internet, and video) get a favored connection over those who just pay for one?

18 Spam, we all know what it is, but there is no proper legal definition on which one can presue a remedy. Let alone from all over the world.

19 <http://www.maawg.org/> Messaging Anti-Abuse working group

20 On close examination, one should really note that its not always the customers fault. Such faults can be traced back to the computer business model offered by Microsoft windows operating systems. You cannot upgrade, or install software without granting "do what you please rights" to the installation software.

21 Exhibit F

22 Exhibit E, Exhibit I

mail. There are some 54 commercial sites that have refused to accept legitimate e-mail based upon Verizon's recommendation²³. How do I, as a consumer, prevent Verizon from degrading my ability to send e-mail. These are all claimed to be the "Best Practices" of the industry. Yet the industry does not include themselves in denial of port 25 access, or blacklisting of their own commercial services. This would, after all, ruin their commercial interests.

Universal Funding

It has been my experience that many ISPs and on-line vendors require access to Credit Card accounts in order to purchase goods and services. Paying by check, money order, or cash (bank transfer) is just not an option by the many businesses that use the internet.

It's just about the same with the FCC. The FCC will only do (small dollar amounts) transactions with businesses that have the capability to accept credit cards. If a business does not have that capability, then the FCC will not do business with them.

Does everyone need a credit card to effectively use the Internet? And are you shut out of that internet business model if one does not have a Mastercharge, or Visa account?

G. Baeslack
Box 446
Stockton, N.J. 08559

Exhibit A

Email AcknowledgementDear Consumer,
Thank you for contacting the Federal Communications Commission (FCC). This is an automated message to confirm that we have received your correspondence. We will review your information to determine how we can best serve you.
If you need to send additional information, you may reply back with this email, leaving the case number (example: CIMS0123456789) in the subject line, or contact us at our toll free phone number 1-888-Call-FCC (1-888-225-5322) and reference the case number.
The Federal Communications Commission

Visit us at our Web Site located at www.fcc.gov, where you will find a wealth of information on a wide variety of communications-related topics.

----- Original Message -----From: netbxxxxx@gatworks.com
Received: 4/26/2010 10:25:44 AM
Subject: What happened to my complaint IC#09-C00165933-1

As of this moment I have yet to hear on my complaint dated November 16, 2009, and received by the FCC on November 23, 2009.

Its not easy to e-mail when Verizon continues to block outgoing Internet port 25 on my broadband account.

I think something is happening, but I have your to get any feedback regarding the disposition of this complaint.

Should I be filing something more formal?

Exhibit B

Subject:

From: "Anna Baughman" <Anna.Baughman at fcc.gov>

Date: Mon, 26 Apr 2010 16:22:42 -0400

To: <netbxxxxx@gatworks.com>

X-Account-Key: account5

X-UIDL: 1272309695.12049.laptopserver.gatworks.com

X-Mozilla-Status: 0003

X-Mozilla-Status2: 10000000

Return-Path: <Anna.Baughman at fcc.gov>

Delivered-To: gatworks-com-netbeans@gatworks.com

Received: (qmail 12047 invoked from network); 26 Apr 2010 19:21:35 -0000

Received: from dmz-mail1.fcc.gov (192.104.54.105) by mail.gatworks.com with SMTP; 26 Apr 2010 19:21:35 -0000

Received: from smarthost2.fcc.gov (gatekeeper4.fcc.gov [192.104.54.21]) by dmz-mail1.fcc.gov (Postfix) with ESMTP id 4FFEE9BB3 for <netbeans@gatworks.com>; Mon, 26 Apr 2010 16:16:41 -0400 (EDT)

Received: from P2PXCS01.fccnet.win.fcc.gov ([165.135.240.143] [165.135.240.143]) by smarthost2.fcc.gov with ESMTP id BT-MMP-222490 for netbeans@gatworks.com; Mon, 26 Apr 2010 16:22:43 -0400

Received: from gbpxcs01v.fccnet.win.fcc.gov ([10.16.144.21]) by P2PXCS01.fccnet.win.fcc.gov with Microsoft SMTPSVC(6.0.3790.4675); Mon, 26 Apr 2010 16:22:43 -0400

Received: from gbpxmb10v.fccnet.win.fcc.gov ([10.16.144.20]) by gbpxcs01v.fccnet.win.fcc.gov with Microsoft SMTPSVC(6.0.3790.4675); Mon, 26 Apr 2010 16:22:42 -0400

X-Brightmail-Tracker: AAAAAQAAAAI=

X-Whitelist: TRUE

X-MimeOLE: Produced By Microsoft Exchange V6.5

Content-class: urn:content-classes:message

Message-ID: <1AF8EFF3A00A6D448182C06390E1320E027FD15C@gbpxmb10v.fccnet.win.fcc.gov>

Thread-Index: Acr1fjmeKenSt8liQbKm1vCUZ57kxQ==

X-OriginalArrivalTime: 26 Apr 2010 20:22:42.0690 (UTC) FILETIME=[39815E20:01CAE57E]

MIME-Version: 1.0

Content-Type: multipart/mixed; boundary="----=_NextPart_001_01CAE57E.39943603"

FCC records indicate that your complaint has been resolved.

I have attached the carrier response from Verizon.

Thank you

Baeslack_09-C00165933[1].pdf

Content-Description: Baeslack_09-C00165933[1].pdf

Content-Type: application/octet-stream

Content-Encoding: base64

1 of 1 07/14/2010 04:08 PM

Exhibit C



December 7, 2009

1717 Arch Street
Floor 17
Philadelphia PA 19107

Complaint

Sharon Bowers
Acting Division Chief
Consumer Inquiries and Complaints Division
Consumer & Governmental Affairs Bureau
Federal Communications Commission
445 12 St., SW
Washington, DC 20554

RE: G Baeslack
Box 446
Stockton NJ 08559
Telephone:
IC Number: **09-C00165933-1**
Received: November 25, 2009

Thank you for referring the complaint of G Baeslack to our office for review. We appreciate the consumer bringing this matter to our attention. The consumer expressed concern with Verizon's internet outbound port 25 blocking.

Please be advised, records do not reflect internet for the consumer. However, per Verizon's Technical Support services, emails were sent to all customers beginning February 2009, to advise of the policy change. The customer's were advised to go to www.verizon.net/port25 for systematic instructions to change the port settings on their computes. In addition, the website explains outbound port 25 blocking, why Verizon is blocking the service and when the change will take effect. According to our website:

What is outbound port 25 blocking?

Outbound port 25 blocking is a network configuration change that will prevent computers on the Verizon network from connecting to servers outside of our network. Servers outside the Verizon network use a method commonly employed to send unauthenticated, unsolicited e-mail or "spam".

Why is Verizon blocking outbound port 25?

The majority of spam (unsolicited email) on the Internet is caused by malicious software viruses that take control of infected computers. These viruses direct the infected machines to send email through port 25. Verizon takes spam very seriously. Verizon blocks outgoing connections on port 25 to prevent infected computers from being used by spammers to send unsolicited email. Outbound port 25 blocking is a standard industry method to control spam.

When will outbound port 25 blocking be implemented?

We will begin implementing outbound port 25 blocking in the first quarter of 2009.

We trust this information will assist you in closing this complaint. We apologize for any inconvenience the consumer has experienced because of the above matter.

Sincerely,

B Lum
Verizon Customer Relations Analyst

cc: G Baeslack

Exhibit D

G. Baeslack
Box 446
Stockton, N.J. 08559
January 28, 2010

Re: IC Number: 09-C00165933-1

To: Sharon Bowers
Acting Division Chief
Consumer Inquiries and Complaints Division
Consumer & Government Affairs Bureau
Federal Communications Commission
445 12 St., SW
Washington, D.C. 20554

Dear Ms Bowers,

I am rather dismayed with the attached reply from B. Lum, Verizon Customer Relations Analyst.

First of all, I have been a Verizon broadband user for some 10 years. Second of all, Verizon has canceled the initial E-Mail address assigned to the broadband account some 10 years ago because of non-usage. For those Verizon E-Mail accounts that Verizon has canceled, it is not clear to me as to how Verizon notified those customers.

The "systematic instructions" to overcome "port 25 blocking" are defective. Verizon e-mail experts are well aware that the instructions will never address the concerns of those providing their own e-mail services.

Verizon claims this is industry practice. Most e-mail experts recognize that the 'industry practice' is only applied to certain broadband classes, and never to the industry itself. Commercial Verizon accounts are not blocked. Verizon e-mail service is not port 25 blocked. It is not clear to me as to why the 'systematic instructions' are not, or has not been foisted upon those accounts, presuming that Verizon is interested in eliminating all potential sources of spam within its walls.

Yes, spam is a big concern to many ISP's. Generally when an infected computer is detected, the owning ISP is notified, and then the client is notified. Generally if the client does not effectively address the issue, then the account is closed. Verizon now wants to apply a broad brush, were as all users of port 25 are convicted irrespective of having an infected computer, or of sending spam.

Verizon does not offer any options for the removal of port 25 blocking. There is a hint that it may be possible, but fails to disclose it.

Verizon does/did offer an e-mail service program for extra monetary fees.

Verizon does not offer any compensation for the loss of port 25.

Its unfortunate that Verizon is unable to effectively manage its e-mail service it provides to its broadband users. Maybe Verizon should drop its e-mail service, just as Verizon recently did with the internet 'newsgroup' service that it once provided. I'm sure that there are e-mail service providers that will be very happy to provide this service to Verizon, and to Verizon customers.

Verizon does not even appear to be worried that their change of policy violates the **Net Neutrality rules of 2005** that the F.C.C. is now trying to codify in rule making. Here Verizon's application (the e-mail service) is being used as an excuse to curtail broadband access. Even today, years after a DOS (Denial Of Service) threat, Verizon decided that blocking incoming port 80 (web/browser services) to be only solution, Verizon has not yet removed that broadband *incoming port 80* block. Verizon also provides those port 80 services, but at an additional cost.

Many knowledgeable professionals can provide their own applications, computer equipment, and policies. What those professionals cannot do is overcome Verizon blocking policies that are designed to protect Verizon own internet applications to the detriment of competing legal, and legitimate user installed applications.

Exhibit E

SPAMHAUS



[Home](#) [SBL](#) [XBL](#) [PBL](#) [DBL](#) [DROP](#) [ROKSO](#)

Blocklist Removal Center

[About Spamhaus](#) | [FAQs](#) | [News Blog](#) | [Site Map](#)

PBL Advisory

Help

[I don't understand what to do about this?](#)

Ref: PBL274558

162.84.80.0/21 is listed on the Policy Block List (PBL)

Associated Documents

- [PBL Home](#)
- [PBL FAQs](#)
- [How Blocklists Work](#)

Outbound Email Policy of Verizon Online for this IP range:

It is the policy of Verizon Online that unauthenticated email sent from this IP address should be sent out only via the designated outbound mail server allocated to Verizon Online customers. To find the hostname of the correct mail server to use, customers should consult the original signup documentation or contact Verizon Online Technical Support.

Removal Procedure

Removal of IP addresses within this range from the PBL is not allowed by the netblock owner's policy.

About The PBL

The Spamhaus Policy Block List ("PBL") is an international anti-spam system maintained by The Spamhaus Project in conjunction with Internet Service Providers and is used by Internet networks to enforce inbound email policies. The PBL database lists end-user IP address ranges which should not be delivering unauthenticated email to any mail server except those provided for specifically for that customer's use. The PBL lists only IP addresses (not domains or email addresses).

For full information on how the PBL operates please see the [PBL Home page](#) and the [PBL Frequently Asked Questions](#).

Exhibit F

An Important Notice from the Los Angeles Superior Court About a Class Action Settlement Involving Verizon Internet Service

If you had Verizon internet service and used your verizon.net mailbox between October 2004 and May 2005, you could get benefits from the settlement.

A proposed settlement has been reached in two class action proceedings alleging that, beginning in October 2004, Verizon blocked legitimate incoming emails to certain Verizon.net subscribers. You may be a member of the Class whose rights are affected by this lawsuit. **The sole purpose of this notice is to inform you of the settlement so that you may decide what steps to take in relation to it.**

If the settlement is approved, Class Members who complete and return a Claim Form on or before October 13, 2006, may be eligible to receive settlement benefits. The Claim Form can be accessed at www.EmailBlockingSettlement.com. You can also obtain the Claim Form by calling the Settlement Administrator toll free at 1-866-730-8147 or by writing the Settlement Administrator, c/o Rust Consulting, Inc., PO Box 1324, Minneapolis, MN 55440-1324. You may also choose to exclude yourself from the settlement and/or object to the settlement.

There are deadlines associated with the choices you may make regarding the settlement. More information on these deadlines and your rights under the settlement, together with instructions for filing a Claim Form, can be obtained at www.EmailBlockingSettlement.com or by contacting the Settlement Administrator at the above phone number or address.

Exhibit G

Email rejection messages from various ISP's

GOOGLE / GMAIL

209.85.212.7_failed_after_I_sent_the_message./Remote_host_said:_421-4.7.0_[151.204.143.76]_Our_system_has_detected_an_unusual_amount_of/421-4.7.0_unsolicited_mail_originating_from_your_IP_address._To_protect_our/421-4.7.0_users_from_spam,_mail_sent_from_your_IP_address_has_been_temporarily/421-4.7.0_blocked._Please_visit_http://www.google.com/mail/help/bulk_mail.html/421-4.7.0 to review our Bulk Email Senders Guidelines. 7si3761008vws.60/

MSN / HOTMAIL

failure: Connected_to_65.55.92.152_but_sender_was_rejected./Remote_host_said:_550_DY-001_Mail_rejected_by_Windows_Live_Hotmail_for_policy_reasons._We_generally_do_not_accept_email_from_dynamic_IP's_as_they_are_not_typically_used_to_deliver_unauthenticated_SSMTP_e-mail_to_an_Internet_mail_server._<http://www.spamhaus.org> maintains lists_of_dynamic_and_residential_IP_addresses._If_you_are_not_an_email/network_admin_please_contact_your_Email/Internet_Service_Provider_for_help._Email/network_admins,_please_visit_<http://postmaster.live.com> for_email_delivery_information_and_support/

YAHOO

Connected_to_66.196.82.7_but_greeting_failed./Remote_host_said:_553_Mail_from_151.204.143.76_not_allowed_-_5.7.1_[BL21]_Connections_not_accepted_from_IP_addresses_on_Spamhaus_PBL;_see_<http://postmaster.yahoo.com/550-bl21.html> 1550/

VERIZON

Connected_to_206.46.232.11_but_greeting_failed./Remote_host_said:_571_Email_from_162.83.226.122_is_currently_blocked_by_Verizon_Online's_anti-spam_system._The_email_sender_or_Email_Service_Provider_may_visit_<http://www.verizon.net/whitelist> and request removal of the block. 090731/

Sorry,_I_wasn't_able_to_establish_an_SSMTP_connection._(#4.4.1)/

HOSTWAYCORP

Connected_to_66.113.135.106_but_greeting_failed./Remote_host_said:_554-mail.chicago.hostwaycorp.com/554_Unfortunately_your_access_to_this_mail_system_has_been_rejected_due_to_the_sending_MTA's_poor_reputation_and_email_hygiene_on_the_Internet._Please_reference_the_following_URL_for_more_information:_<http://www.senderbase.org/search?searchString=162.83.255.206/>

EBAY

Connected_to_66.135.195.181_but_greeting_failed./Remote_host_said:_554-data.ebay.com/554_BLACKLIST/

QMAIL

131.193.36.27_does_not_like_recipient./Remote_host_said:_451_http://www.spamhaus.org/query/bl?ip=151.204.141.92/Giving_up_on_131.193.36.27/

AOL

Connected_to_205.188.158.56_but_greeting_failed./Remote_host_said:_554-(RTR:DU)_http://postmaster.info.aol.com/errors/554rtrdu.html/554_Connecting_IP:_151.204.143.76/

Exhibit H

Organizations that blacklist based in IP address.

1. Outblaze, Limited, 10 Marshall Street, Old Greenwich, CT, 06870
2. Global Crossing, 14605 South 50th Street. Phoenix. AZ. 85044-6471.
3. The Pennsylvania State University , 105 USB 2, University Park, PA, 16802.
4. Silicon Graphics, Inc., 1500 Crittenden Lane, Mountain View, CA, 94043
5. TelePacific Communication, 515 South Flower St. 47th Floor, LOS ANGELES, CA, 90071
6. **AT&T WorldNet Services**, AT&T, 200 S. LAUREL AVE., MIDDLETOWN, NJ, 07748
7. **Comcast Cable Communications**, Inc., 1800 Bishops Gate Blvd, Mt Laurel, NJ, 08054,
8. **AT&T Internet Services** , 2701 N. Central Expwy # 2205.15, Richardson, TX, 75080
9. CERFnet, 5738 Pacific Center Blvd, San Diego, CA, 92121
10. iPowerWeb, Inc., 2800 28th Street Suite 205, Santa Monica, CA, 90405
11. **GE Corporate**, Network Administrator, 1 Independence Way, Princeton, NJ, 08540
12. **Hewlett-Packard Company**, 3000 Hanover Street, Palo Alto, CA, 94304
13. MPOWER COMMUNICATIONS CORP., 175 SULLY'S TRAIL, SUITE 350, PITTSFORD, NY, 14534
14. Hughes Network Systems, 11717 Exploration Lane, Germantown, MD, 20876
15. Optimum Online (Cablevision Systems), 111 New South Road, Hicksville, NY, 11801
16. McLeodUSA Incorporated, 6400 C Street SW, PO Box 3177, Cedar Rapids, IA, 52406
17. Collabnet, 8000 Marina Blvd., Suite 600, Brisbane, CA, 94005
18. Cablevision Systems Corp., 1111 Stewart Avenue, Bethpage, NY, 11714
19. PenTeleData Inc., 540 Delaware Ave., Palmerton, PA, 18071
20. Wave Broadband, LLC, 401 Kirkland Park Place, Suite 313, Kirkland, WA, 98033
21. Dell Computer Corporation, One Dell Way, Round Rock, TX, 78682
22. Wake Forest University, P. O. Box 7408, Reynolda Station, Winston-Salem, NC, 27109
23. PATRIOT MEDIA AND COMMUNICATIONS, LLC, 100 Randolph Road, Somerset, NJ, 08873
24. Silver Star Telecom, LLC, 16420 SE McGillivray, Suite 103-233, Vancouver, WA, 98683
25. Hawaiian Telcom, 1177 Bishop St., Honolulu, HI, 96813
26. MessageLabs Inc., 512 Seventh Avenue, 6th Floor, New York, NY, 10018
27. VA Software, 46939 Bayside Parkway, FREEMONT, CA, 94538
28. **Google Inc.**, 1600 Amphitheatre Parkway, Mountain View, CA, 94043
29. **Cox Communications Inc.**, 1400 Lake Hearn Drive, Atlanta, GA, 30313
30. Frontier Communications of America, Inc., 180 South Clinton AVE, Rochester, NY, 14646
31. Hawaiian Telcom Services Company, Inc., 1177 Bishop St., Honolulu, HI, 96713
32. **Sprint**, 12502 Sunrise Valley Drive, Reston, VA, 20196
33. **Comcast Cable Communications**, Inc., 1800 Bishops Gate Blvd, Mt Laurel, NJ, 08054,
34. Lockheed Martin Corporation, 1401 Del Norte, Denver, CO, 80221
35. Creative Computers, 2555 W. 190th Street, Torrance, CA, 90504
36. **Clearwire, LLC**, 5808 Lake Washington Blvd NE, Suite 300, Kirkland, WA, 98033
37. Global Telecom, INC (GTI), 33 Market Street, 2nd Floor, Morristown, NJ, 07960
38. WACHOVIA CORP, 809 W 4.5 ST, WINSTON-SALEM, NC, 27102
39. **Trend Micro**, Inc., 10101 N. De Anza Blvd., Cupertino, CA, 95014

40. **Symantec Corporation**, 20330 Stevens Creek Blvd, Cupertino, CA, 95014
41. Outblaze, Limited, 10 Marshall Street, Old Greenwich, CT, 06870
42. The Pennsylvania State University , 105 USB 2, University Park, PA, 16802.
43. **America Online**, 22000 AOL Way, Dulles, VA, 20166
44. ThePlanet.com Internet Services, Inc., 315 Capitol, Suite 205, Houston, TX, 77002
45. **EarthLink Network**, Inc., 1375 PEACHTREE ST, LEVEL A, ATLANTA, GA, 30309
46. **XO Communications**, Corporate Headquarters, 11111 Sunset Hills Road, Reston, VA, 20190-5339
47. Co-Location.com Inc., Wholesale Internet Division, 333 S. Beverly Drive, Suite 105, Beverly Hills, CA, 90212
48. **Go Daddy Software**, Inc., 14455 N Hayden Road, Suite 226, Scottsdale, AZ, 85260
49. **Disney Worldwide Services**, Inc., 500 South Buena Vista Street, Burbank, CA, 91521
50. **BellSouth.net Inc.**, 575 Morosgo Drive, Atlanta, GA, 30324
51. Domain Name Holding Company, Inc, 70 Blanchard Rd., Burlington, Massachusetts 01803
52. **Microsoft Corp**, One Microsoft Way, Redmond, WA, 98052
53. **eBay**, Inc, 2145 Hamilton Ave, San Jose, CA, 95008
54. AltaVista Company,**Yahoo**, 701 First Ave, Sunnyvale, CA, 94089

Exhibit I

<http://www.spamhaus.org/pbl/query/PBL274489>



Ref: PBL274489

151.204.128.0/19 is listed on the Policy Block List (PBL)

Outbound Email Policy of Verizon Online for this IP range:

It is the policy of Verizon Online that unauthenticated email sent from this IP address should be sent out only via the designated outbound mail server allocated to Verizon Online customers. To find the hostname of the correct mail server to use, customers should consult the original signup documentation or contact Verizon Online Technical Support.

Removal Procedure

Removal of IP addresses within this range from the PBL is not allowed by the netblock owner's policy.

About The PBL

The Spamhaus Policy Block List ("PBL") is an international anti-spam system maintained by The Spamhaus Project in conjunction with Internet Service Providers and is used by Internet networks to enforce inbound email policies. The PBL database lists end-user IP address ranges which should not be delivering unauthenticated email to any mail server except those provided for specifically for that customer's use. The PBL lists only IP addresses (not domains or email addresses).

For full information on how the PBL operates please see the [PBL Home page](#) and the [PBL Frequently Asked Questions](#)