

July 29, 2008

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: Ex Parte Communication, WC Docket No. 07-52, Network Management Practices

Dear Ms. Dortch:

As you know, the Commission has announced its intention to take action on the abovementioned matter at its upcoming meeting.

The Commission has not issued a Notice of Proposed Rulemaking in this matter, as is normally the case when it imposes sweeping new restrictions upon an industry. Rather, its action appears to be based upon a vague and ambiguous policy statement – a list of “principles” which had been presented to the public as unenforceable. Furthermore, many if not most of the points of this policy statement appear to be in direct conflict with the policy which was set into statute by Congress at 47 USC § 230(b), which would be expected to take precedence.

This development has left the public in confusion as to what constraints – written or unwritten – the Commission might intend to apply to Internet service providers. This confusion has deterred investment in broadband deployment and has severely damaged the business prospects of some manufacturers of network equipment. The potential harm to small, rural and wireless ISPs is particularly great.

In an attempt to limit the damage that this uncertainty will do to ISPs, to Internet deployment or to equipment manufacturers, I have e-mailed the attached list of 20 questions to the chief aide of each of the Commissioners. Because this constitutes a material ex parte communication regarding the proceeding, I am also filing a copy for public inspection via the Commission's Electronic Comment Filing System, as required by Section 1.1206(b)(2) of the Commission's rules.

It is my hope that, when they see the wide range of questions raised by their forthcoming action, the Commissioners and their staffs will be encouraged to furnish answers as part of the ruling, thereby clarifying what it bodes for the abovementioned industries. If they fail to do so, both of these industries may be indefinitely hobbled by confusion as to what the Commission's desired “rules” for the Internet might be.

Sincerely,

/s/

Laurence Brett (“Brett”) Glass, d/b/a LARIAT
PO Box 383
Laramie, WY 82073-0383

cc: Daniel Gonzalez, Rick Chessen, Scott Bergmann, Amy Blankenship, Angela Giancarlo

Twenty Questions for the FCC Regarding Network Management

by Laurence Brett ("Brett") Glass, d/b/a LARIAT

1. I operate a public Internet kiosk which, to protect its security and integrity, has no way for the user to insert or connect storage devices. The FCC's policy statement says that a provider of Internet service must allow users to run applications of their choice, which presumably includes uploading and downloading. Will I be penalized if I do not allow file uploads and downloads on that machine?
2. I am a librarian. Our library operates a public computer which, for security reasons, only allows the user to run certain applications -- e.g. a Web browser and games. To maintain quiet, we have also disabled its sound card. Because it offers service to the public but blocks audio media and does not allow the user to run any application, is it in violation of the FCC's rules or policies?
3. I am a network administrator for a university which provides Internet to students, faculty, and staff throughout campus (including the dormitories and campus apartments where students -- and, in the case of the apartments, their spouses and children -- live). Like most universities, we charge fees for access in the residences and thus act as a commercial ISP in those locations. We currently prohibit P2P traffic and use a dedicated P2P mitigation appliance to block it. If we did not, P2P would consume all of our bandwidth, invite lawsuits from intellectual property owners whose works are being pirated, and violate the terms of grants which fund our acquisition of Internet bandwidth (which state that it must be used only for certain purposes). Are we in violation of FCC rules if we continue P2P blocking? Do we need to discontinue it in the dormitories and apartments, where we serve as a residential ISP? What about the public Wi-Fi we maintain in locations such as the Student Union?
4. I operate a wireless hotspot in my coffeehouse. I block P2P traffic to prevent one user from ruining the experience for my other customers. Do the FCC rules say that I must stop doing this?
5. I own an apartment building which provides free wireless Internet to tenants as an incentive to rent. I have contracted with my ISP to block P2P traffic so that one or a few tenants cannot monopolize the bandwidth and cause complaints by other tenants, and also to avoid liability for copyright violations. I do tell my tenants what I am doing and why. May I continue to do this under FCC policy? May my ISP?
6. I am a cellular carrier who offers Internet services to users of cell phones. Due to spectrum limitations, multimedia streaming by more than a few users would consume all of the bandwidth we have available not only for data but also for voice calls. May we restrict these protocols to avoid running out of bandwidth and to avoid disruption to telephone calls (some of which may be E911 calls or other urgent traffic)?
7. I am a wireless ISP operating on unlicensed spectrum. Because the bands are crowded and spectrum is scarce, I must limit each user's bandwidth and duty cycle. Rather than imposing hard

limits or overage charges, I would like to set an implicit limit by prohibiting P2P, with full disclosure that I am doing so. Is this permitted under the FCC's rules?

8. I am a rural ISP who pays \$500 per megabit per second per month for bandwidth. The use of P2P would make it impossible to offer affordable service to my customers. May I prohibit P2P on residential class connections, with full disclosure that I am doing so and that the user can upgrade to a "business class" connection which allows P2P?

9. I am an ISP who serves a school which is required, by COPA, to block certain content, including entire Web sites. We provide this blocking for them as a service. Is this a violation of the FCC's rules?

10. My hotel offers Internet access to guests. We block outbound connections on TCP Port 25 (unencrypted, unauthenticated e-mail) so that guests, or others who enter the hotel, cannot send spam either intentionally or unintentionally (for example, if their machines are infected with a "Trojan Horse" program). We could have our Internet connection cut off, or our Internet address blacklisted, if we do not do this. Will we have to stop this in light of the FCC's ruling?

11. We run an ISP. We block the TCP ports used by Windows messaging (used for unsolicited pop-up messages, which have never been declared to be illegal but are annoying). We also block outbound connections on some other ports, such as TCP Port 25, to avoid being blacklisted by the Internet or having our service cut off by our upstream provider. We also block the TCP ports used by Windows networking so that a user does not inadvertently share his or her files with the entire Internet. Are these restrictions, which are generally considered to be "best practices" for ISPs, contrary to the FCC's policy?

12. I operate an ISP which, like most, has a limited number of Internet addresses, and so uses Network Address Translation (NAT) for many of its customers. This allows many customers to share a single IP address and also protects the customers from many Internet attacks. However, NAT does prevent customers from running a server. If we had to give every user a unique public IP address, it would raise our costs and expose our users to security risks. Does the FCC policy which mandates that users be allowed to run any application require us to obtain a unique, public IP address for every subscriber? (Note that if this were the case, ISPs throughout the country would have to obtain so many new addresses that the supply of IP Version 4 addresses would likely be exhausted.)

13. I operate an Internet hotspot at an airport which does Network Address Translation (as most Wi-Fi routers do) and therefore does not allow users to run servers. It isn't appropriate for hotspot users at an airport to be running servers, but the FCC seems to be requiring that we allow them to run any application. Must we stop doing network address translation, acquire public IP addresses at substantial extra cost, expose users to direct threats from the Internet from which NAT would protect them, and expose our network to potential congestion by users running servers?

14. I am an ISP that accelerates users' Web browsing by rerouting requests for Web pages to a Web cache (a device which speeds up Web browsing, conceived by the same people who developed the World Wide Web) and then to special Internet connections which are asymmetrical (that is, they have more downstream bandwidth than upstream bandwidth). The result is faster and more economical Web browsing for our users. Will the FCC say that our network "discriminates" by handling Web traffic in this special way to improve users' experience?

15. We are an ISP that improves the quality of VoIP by prioritizing VoIP packets and sending them through a different Internet connection than other traffic. This technique prevents users from experiencing problems with their telephone conversations and ensures that emergency calls will get through. Is this a violation of the FCC's rules?

16. We're an ISP. A user on our network is running a "port scanner" – a program which scans other computers on the network for potential vulnerabilities. This application is not in and of itself illegal, but our policy prohibits it because port scans are invasive and are usually a prelude to a hacker attack. (Virtually all automated intrusion detection systems to block Internet hosts that are engaging in port scanning to prevent computers from being integrated into "botnets.") We want to protect other users' security and privacy. Does our prohibition on port scanning run afoul of the Commission's requirement that we allow users to run any application?

17. We are an ISP that wants to protect users from "spyware" and "adware," and therefore block sites where such annoying software resides. In many cases, this software is not explicitly illegal, though perhaps it should be. And in some cases, the software appears to offer a useful service to the user but may be exploiting him or her by, for example, gathering personal data, popping up ads, or redirecting Web browsing. Could we be penalized for protecting our users from this annoying and sometimes malicious software by blocking it?

18. We're an ISP that serves several large law offices as well as other customers. We are thinking of renting a direct "fast pipe" to a legal research database to shorten the attorneys' response times when they search the database. Would accelerating just this traffic for the benefit of these customers be considered "discrimination?"

19. We're a wireless ISP. Most of our customers are connected to us using "point-to-multipoint" radios; that is, the customers' connection share a single antenna at our end. However, some high volume customers ask to buy dedicated point-to-point connections to get better performance. Do these connections, which are engineered by virtually all wireless ISPs for high bandwidth customers, run afoul of the FCC's rules against "discrimination?"

20. Our company provides satellite broadband service. The bandwidth of our satellites is limited, and so we prohibit P2P traffic and throttle it back or block it if we see it. In many remote rural areas, ours is the only service other than dialup that is available. If we do not mitigate P2P, our service will become unreliable or unavailable, and many rural users will be cut off from any high speed service. Does the recent ruling mean that we can no longer prohibit, throttle, or block P2P?