

BEFORE THE
Federal Communications Commission
WASHINGTON, D.C.

| | | |
|------------------------------|---|----------------------|
| In the matter of |) | |
| |) | |
| Preserving the Open Internet |) | GN Docket No. 09-191 |
| |) | |
| Broadband Industry Practices |) | WC Docket No. 07-52 |
| |) | |

**COMMENTS OF LAURENCE BRETT (“BRETT”) GLASS,
d/b/a LARIAT, A WIRELESS INTERNET SERVICE
PROVIDER SERVING ALBANY COUNTY, WYOMING**

Laurence Brett (“Brett”) Glass, a sole proprietor doing business as LARIAT, a wireless Internet service provider serving Albany County, Wyoming, responds to the Notice of Proposed Rule Making issued by the Commission on October 22, 2009¹ with the following comments.

1. INTRODUCTION AND EXECUTIVE SUMMARY

LARIAT was among the first, if it was not the very first, of the wireless Internet service providers (WISPs) now doing business within the continental United States. LARIAT provides high quality, high speed broadband Internet service to a large and growing service area in rural Wyoming. LARIAT was originally founded as a nonprofit, 501(c)(12) rural telecommunications cooperative, and was taken private by its founder, Brett Glass, at the request of the membership in 2003.

While it is now a for-profit business, LARIAT has maintained the same consumer friendliness, transparency, and “no nonsense” business practices that it had as a co-op. LARIAT has never censored

¹ *Preserving the Open Internet; Broadband Industry Practices*, Federal Communications Commission, Notice of Proposed Rule Making, GN Docket No. 09-191, WC Docket No. 07-52, FCC Rcd. 13064 (2009) (“NPRM”)

lawful Internet content – nor would it ever do so – and fiercely guards its users’ privacy. Users appreciate the opportunity to receive service from a local provider which creates jobs in the community, supports community organizations (e.g., via free Web hosting for local nonprofits), and provides local technical support rather than forwarding calls to offshore call centers.

In pursuit of its mission to bring high speed Internet to unserved and underserved areas, LARIAT now expands its service area by approximately the size of the District of Columbia every year. LARIAT does this by employing innovative engineering practices, constantly combating rising levels of interference on the unlicensed (Part 15) bands to bring quality service to remote areas.

Despite its small size, limited capitalization, inability to obtain exclusively licensed spectrum, and dependence upon anticompetitively priced “special access” lines for its connection to the Internet backbone, LARIAT not only serves outlying areas but also competes gamely with much larger providers – including Bresnan Communications and Qwest – in the areas of Laramie which they serve. It is also engaged in vigorous competition with cellular data providers, satellite providers, and three non-local WISPs which have entered the market in Laramie. (Laramie has at least 9 other facilities-based providers, as well as an additional handful of non-facilities-based providers which deliver service via Qwest’s infrastructure.)

The abovementioned spectrum limitations and economic constraints require LARIAT, like other WISPs, to be innovative not only in its technology but also in its business models and practices. Rate plans and terms of service are structured to reflect actual costs, and pricing is aggressive; the typical profit from a residential account is no more than \$2.50 per month. (Because LARIAT provides 24x7 support by transferring calls to technicians cell phones, LARIAT may lose money on the account if a customer makes even one technical support call per month.)

Unfortunately, the rules in the present NPRM would prohibit LARIAT’s most popular and consumer-friendly residential rate plans, raising prices to consumers. The rules would also hinder LARIAT’s ability to maintain good quality of service over the limited amount of cluttered, unlicensed spectrum available to it. By increasing costs, they would also limit LARIAT’s ability to deploy new

service to currently unserved and underserved areas, hampering competition and limiting consumers' broadband choices. While purporting to address problems that do not yet exist and are exceedingly unlikely ever to exist, the proposed rules – unlike the FCC's original "Internet Policy Statement"² – would fail to address some actual market failures and anticompetitive practices. (Incumbent local exchange carriers and some Internet content providers – including eBay, Google, YouTube, and ESPN360 – do have market power and have engaged in horizontal and vertical monopoly leverage.)

The proposed rules have also frightened potential investors in LARIAT's business. Currently, LARIAT is entirely self-financed, except for a small business credit line. What's more, due to the bank's lack of confidence that small, independent providers will be able to survive potential regulation and anticompetitive practices by incumbents, even this credit line is secured not by the assets of the business but by the owner's personal real estate holdings. The imposition of regulations that would drive up costs or hamper innovation would further deter future outside investment in our company and others like it.

For these reasons, LARIAT respectfully requests that the Commission follow Hippocrates' maxim – "First, do no harm" – and adopt at most two simple and unambiguous rules rather than the six enumerated in the NPRM. The first of these should prohibit anticompetitive business practices, such as blocking or hindering the delivery of services (e.g., "over the top" VoIP) that compete with those provided by the ISP itself. It should also prohibit the pricing of wholesale Internet services so as to forestall competition at the retail level ("price squeezing"), as has currently been implemented via excessive "special access" pricing. This first rule should not be limited to ISPs, but – in keeping with the fourth principle

²*Appropriate Framework for Broadband Access to the Internet over Wireline Facilities; Review of Regulatory Requirements for Incumbent LEC Broadband Telecommunications Services; Computer III Further Remand Proceedings; Bell Operating Company Provision of Enhanced Services; 1998 Biennial Regulatory Review – Review of Computer III and ONA Safeguards and Requirements; Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities Internet Over Cable Declaratory Ruling; Appropriate Regulatory Treatment for Broadband Access to the Internet Over Cable Facilities*, Policy Statement, 20 FCC Rcd 14986, 14987–88, para. 4 (2005) ("Internet Policy Statement").

enumerated in the original Internet Policy Statement³ – should also be applicable to any provider of Internet content or services with substantial market power.

The second rule should mandate transparency, so that consumers of Internet service are able to make informed and valid comparisons between the services which are available to them. Users should know before subscribing if certain network behaviors are prohibited or constrained, how traffic is managed, whether surcharges are imposed for heavy resource usage, and – to an extent that will not compromise security – how security measures such as blocking of vulnerable TCP ports are implemented and if they may be overridden.

By fostering competition, these two rules would enable robust markets, thereby making it unnecessary to impose any other rules to preserve an “open” Internet. They would also avoid the deleterious consequences that would arise from micromanagement of ISPs or prohibition of innovative practices.

2. THE INTERNET WAS DESIGNED, FROM THE OUTSET, TO ALLOW DIVERSE ACCEPTABLE USE POLICIES AND BUSINESS MODELS

The Internet was made possible by the adoption of a set of protocols –TCP/IP – which allowed autonomous networks owned and administered by different entities to exchange data. One reason why the Internet was able to grow and develop into the vast, worldwide resource we know today is that it did not require those networks to have similar topologies, technologies, terms of service, or codes of conduct; all they needed to do is speak TCP/IP, the *lingua franca* of the Net. As a result, it became possible for educational institutions, government agencies, private companies, and – ultimately – commercial Internet

³“To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to competition among network providers, application and service providers, and content providers.” *Ibid*, p.3.

service providers to exchange data. Needless to say, the appropriate acceptable use policies⁴ for these entities are vastly different. Schools, for example, have policies prohibiting academic dishonesty or misuse of resources; corporations and government agencies restrict their networks to official uses and prohibit the dissemination of proprietary or classified information; Internet service providers have terms of service prohibiting excessive consumption of resources. Had the Internet required all of the entities that participated in it to adopt identical AUPs, many if not most of these entities would have opted out and the Internet as we know it would never have come into existence.

By the same token, providers of Internet service – be they academic institutions, commercial ISPs, hotels, coffeehouses, etc. – should, and must, be able to adopt uniquely tailored rules of behavior and business models for their networks. There is not, and we should not mandate that there be, a “one size fits all” model for Internet service.

Unfortunately, the proposed rules limit network owners to but a single criterion for whether behavior on a network is acceptable: that of “lawfulness.”⁵ Any behavior that is not explicitly prohibited by law – no matter how disruptive – is presumptively allowed, unless the operator’s prohibition is deemed to fall into the vaguely defined category of “reasonable network management.”

Because there is already robust competition among ISPs even in remote locations such as Laramie (a small college town of 28,000 souls), and because the FCC has the power to promote even more competition by prohibiting anticompetitive practices, it is far better to encourage diversity among network providers’ policies and allow the market to choose which is best. To mandate overly permissive network management policies would foster lower quality of service, raise operating costs (which in turn would raise prices for all subscribers), and/or create a large backlog of adjudicative proceedings at the Commission (in which it would be prohibitively expensive for small and competitive ISPs to participate).

⁴ For a more complete discussion of network AUPs, or Acceptable Use Policies, see Wikipedia at http://en.wikipedia.org/wiki/Acceptable_use_policy

⁵ See NPRM, P. 38

3. THE PROPOSED RULES WOULD PROHIBIT LARIAT’S MOST POPULAR, ECONOMICAL, AND CONSUMER-FRIENDLY RATE PLANS

Another (probably unintended) consequence of the proposed rules is that they would prohibit innovative rate plans that are popular with consumers and which foster broadband adoption. Because, to date, the Commission has enacted no remedy for the anticompetitive “special access” charges which drive LARIAT’s wholesale cost of Internet bandwidth to upwards of \$100 per Mbps per month. (Despite the decreasing cost of bandwidth in urban areas, this cost has not decreased over the past several years; as backbone providers have dropped their prices, per-megabit charges from the ILECs have actually increased.) Some WISPs in even higher cost areas pay as much as \$300 per Mbps per month for bandwidth. Nonetheless, LARIAT offers a “budget” tier of residential broadband service, with performance that is acceptable to most consumers, for only \$30 per month.⁶ LARIAT is able to do this by buying asymmetrical bandwidth, which is less expensive than symmetrical bandwidth, to provision residential services. It then ensures that the traffic is actually asymmetrical by prohibiting, by contract, the operation of servers – including P2P nodes – on those connections. (“Business class” connections, on which servers are allowed, are also available, though at higher cost.) Customers willingly accept this minor constraint in exchange for economically priced service, knowing that they can buy “business class” service or upload content to any number of inexpensive hosting services if they wish to serve content.

None of the constraints on such connections in any way inhibits political participation, free speech, or access to content. In fact, because LARIAT is able to buy more downstream bandwidth for the user, he or she has access to content which would not be otherwise be viewable in real time. These rate plans likewise foster broadband adoption and encourage users to migrate from dialup service by keeping high speed connections affordable. Because the market has indicated a desire for such classes of service, the Commission would be doing a disservice to consumers – and, in fact, making the Internet less “open” – if it

⁶ For a list of LARIAT’s current asymmetrical residential and small business rate plans, see <http://www.lariat.net/rates.html>.

were to prohibit this and similar business models.

4. THE PROPOSED RULES WOULD PRECLUDE INNOVATIVE, CONSUMER-FRIENDLY SERVICE AND PAYMENT MODELS

Besides prohibiting LARIAT's most popular existing offerings, the proposed rules would also prohibit innovative business and payment models that consumers would likely appreciate. For example, many of LARIAT's customers engage in activities that consume large amounts of bandwidth – for example, viewing a high definition Netflix video – only occasionally during in a given week or month. These consumers do not wish to upgrade to a higher tier of service just to be able to watch these shows. They also do not want to be charged by the hour or day for extra bandwidth; in fact, they enjoy our company's no-nonsense “flat rate” billing (which is 100% predictable – no surprises! – and allows them to schedule automatic, fixed payments via their banks' bill paying services).

One answer to this conundrum would be to allow an advertiser to buy additional bandwidth – and/or higher quality of service – for the consumer for the duration of a program, in exchange for being able to reach the user with an advertisement before the program began. (The charge to the advertiser might be a dollar or two – an amount similar to that charged by Google for a “click-through” on a popular search term – and would cover the ISP's costs.) Such an arrangement would be a “win” for all concerned. The consumer would get the extra bandwidth he or she needed to enjoy the program; the advertiser would reach an appreciative consumer who knew that the program was truly “brought to you” by the advertiser; the content provider would be able to reach the customer with higher quality content; and the ISP would generate extra cash flow without inconveniencing the customer.

Unfortunately, this sort of “spot priority” (or “spot bandwidth”) would be prohibited by the proposed rules, which explicitly state that the ISP cannot allow a third party to pay for an expedited or enhanced connection for the consumer. The result would be to impose – needlessly – far more awkward payment models in which the consumer paid a premium (perhaps entering a credit card number or finding

an extra charge on his or her bill) or had to upgrade to a more expensive service tier.

This is but one example of an innovative and useful service which would be precluded by rules which, without good cause, prohibited business models that might be useful to consumers. Virtually all businesses – from airlines to package delivery services to railroads to theaters – charge not only for services but for priority or enhanced services. Just as the existence of UPS Red or FedEx overnight service does not give Amazon a leg up on smaller online retailers, the ability to purchase prioritization, lower latency, lower jitter, or other quality of service enhancements would not – as some commenters have claimed without substantiation – disadvantage smaller providers of Internet content or services. In fact, to prohibit the sale of such services might in fact preclude innovative services which have special quality of service requirements from being deployed at all – to the detriment of consumers.

5. WIRELESS IS DIFFERENT

Another problematic provision of the proposed rules provides that ISPs may not “prevent any of its users from connecting to and using on its network the user’s choice of lawful devices that do not harm the network.”⁷ This provision would create problems for wireless providers such as LARIAT for several reasons. Besides precluding the ISP from offering more favorable rates for connections that do not allow the operation of servers (see above), it would prevent wireless ISPs, in particular, from insisting that the user’s equipment be properly engineered to meet the requirements of the network – with potentially serious results. Many portions of LARIAT’s network, for example, use equipment which conforms to the IEEE’s 802.11g standard. Should a user connect a radio to a badly aimed antenna, or one with insufficient gain, the network will slow down as it attempts to accommodate the “weak” node. Worse still, if the user attempts to use equipment which conforms to the earlier 802.11b standard, the 802.11g access point will “step down” to a backward-compatible mode in which it drops to 10% or less of its normal capacity. To maintain good

⁷ See NPRM, P. 38.

quality of service, LARIAT insists that all equipment that uses the network be specified and installed by us. Without this requirement, we could not provide adequate quality of service on unlicensed spectrum (which is extremely noisy even in small towns such as Laramie).

Shannon's Law limits the throughput that can be obtained from the congested unlicensed spectrum. Therefore, LARIAT must likewise prohibit the use of applications and devices which attempt to consume all of the network's capacity. Some radio equipment has the ability to "rein in" such applications so that they are unable to degrade the network. But other equipment – especially the most economical outdoor wireless radios – does not have this capability. To foster broadband adoption, users should be allowed to opt for less expensive equipment if they agree not to run applications which congest the network.

6. 20 QUESTIONS

The sweeping rules in the NPRM raise numerous questions about their applicability to different situations. Do they apply to broadband Internet service in airports? Coffeehouses? Apartment buildings? Motels? Universities (which, in fact, have larger networks with more customer revenue than many private ISPs)? Does it matter – or should it – whether the user pays a separate fee for the service or whether it is included in the cost of, say, a hotel room? Who constitutes a "provider of broadband service?" When do network management practices cross the line from being "reasonable" to being "unreasonable?" To illustrate just some of the many questions raised by the proposed rules, Appendix A of this comment contains a list of "20 questions" regarding different situations, and businesses, to which the proposed rules might be applied. We urge the Commission to consider not just these specific questions but their larger implications – in particular, their potency as an argument for simple rules that stimulate competition rather than micromanaging technology businesses and their business models.

7. CONCLUSION

In a 2006 speech,⁸ then-Senator Barack Obama pledged to support “network neutrality” – which he defined as the elimination of “barriers to entry” caused by anticompetitive conduct. It is tempting for the Commission to try to accomplish this via highly prescriptive rules. However, the most likely outcome such an approach would be to destroy competition and hinder innovation, thus harming consumers. It may also exceed the powers granted to the Commission by statute⁹. A more enlightened approach that would fulfill the President’s promise – and would indisputably lie within the FCC’s power – would be to draft rules which, instead of shackling ISPs, prohibit anticompetitive tactics and promote transparency to consumers. LARIAT respectfully recommends that the Commission adopt this approach so as to avoid jurisdictional issues as well as the deleterious consequences that would likely result from the rules as presented in the NPRM.

Respectfully submitted,

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

⁸ Text and audio available at <http://www.obamaspeeches.com/076-Network-Neutrality-Obama-Podcast.htm>

⁹ See, for example, *CES: FCC Commissioners Pessimistic on Net-Neutrality Prospects?* Schatz, Amy, <http://blogs.wsj.com/digits/2010/01/09/ces-fcc-commissioners-pessimistic-on-net-neutrality-prospects/>

APPENDIX A

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?