

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
)	

**REPLY COMMENT OF LAURENCE BRETT (“BRETT”) GLASS,
d/b/a LARIAT, A WIRELESS INTERNET SERVICE
PROVIDER SERVING ALBANY COUNTY, WYOMING,
REGARDING REASONABLE NETWORK MANAGEMENT AND
HANDLING OF UNWANTED CONTENT**

On January 12, 2010, members of the Commission met with representatives of private industry and advocacy groups as part of the Technical Advisory Process (TAP) in the above captioned proceedings.¹ Laurence Brett (“Brett”) Glass, a sole proprietor doing business as LARIAT, a wireless Internet service provider serving Albany County, Wyoming, was not present at the meeting and is therefore responding to the summary of the meeting included in the OET’s Notice of Ex Parte Communication with the following comments.

1. INTRODUCTION

LARIAT, which has operated continuously for 18 years as a broadband Internet service provider, has from its inception found it necessary to deal with the problems of network abuse and unwanted content. From the earliest days of the Internet – when spammers exploited “open mail relays” to send unsolicited

¹ See OET January 14, 2010 Notice of Ex Parte Communication, GN Docket No. 09-191 and WC Docket No. 07-52.

commercial e-mail – LARIAT has employed, and published technical information about, practical measures to block spam, malware, and other threats. It has also participated in the development of industry best practices to achieve these ends.²

Unfortunately – and, probably, unintentionally – the rules proposed in the above captioned matter,³ if adopted as proposed, would prevent ISPs from engaging in some of these desirable and necessary best practices. These rules may also preclude effective responses to new threats or nuisances that might crop up in the future. The purpose of this reply comment is to highlight some of these potential problems and recommend Commission actions which would avoid such unfortunate consequences.

2. SPAM, “BOTNETS,” AND DNS “BLACKLISTS”

In the early days of the Internet, unsolicited commercial e-mail, or “spam,” was most often sent by mail servers specifically set up for that purpose by the sender of the spam. (For example, the infamous spammer Sanford Wallace, also known as “Spamford,” sent spam from the domain “cyberpromo.com”.) Such spam was relatively easy to block – as mentioned in the technical paper cited above – by configuring one’s mail server to block messages originating from specific domains.⁴

Nowadays, spammers only occasionally use their own machines to send spam. More frequently, they harness the computers of innocent Internet users throughout the global Internet to do their dirty work. Spammers exploit security vulnerabilities to commandeer users’ computers, turning them into an army of “spambots.” These machines, in turn, transmit the unsolicited e-mail to the rest of the world. Tracking down and disabling the “botnets,” or maintaining lists of the “zombies” or “spambots” which comprise

² See, for example, *Stopping Spam and Malware with Open Source*, Glass, Brett, O’Reilly Open Source Conference, July 27, 2001. Slides and paper available at <http://www.brettglass.com/spam/>.

³ *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”).

⁴ Glass, Brett, *Op. cit.*

them, is an arduous task that no individual ISP could undertake on its own. So, now that more than 87.7% of all attempted e-mail transmissions on the Internet are spam⁵ – as much as 93.8 percent in some parts of the US⁶ – ISPs must use “blacklists” compiled by third parties to prevent their e-mail systems from being overwhelmed by incoming spam. Many of these lists are cooperative efforts and/or non-profits funded by contributions from ISPs worldwide.

LARIAT uses several popular blacklists, including those maintained by Spamhaus,⁷ to block spam. It also blocks mail from machines with dynamically assigned IP addresses – a characteristic which legitimate mail servers, by convention, do not have. It likewise blocks incoming mail from servers which do not fully conform to the SMTP standard. (The software run by “spambots” often violates the standard in an attempt to send spam as quickly as possible.) And, finally, it blocks mail from a list of offshore networks which are known to host spammers. Overall, 80% to 90% of all attempts to send e-mail to LARIAT’s servers are recognized as spam and blocked.⁸

It is worth noting that users’ appraisals of LARIAT’s system have been uniformly positive. Users thank us for the effectiveness of our spam blocking, and there has been only one reported incident of inadvertent blocking of desired e-mail in the past three years. (This mail, as it turned out, was being sent via a Microsoft Exchange server which had been compromised and was, indeed, a member of a “botnet.”)

3. BLOCKING OF UNAUTHENTICATED OUTBOUND E-MAIL (SMTP)

Needless to say, ISPs not only must carefully evaluate the validity of those blacklists – choosing

⁵ See *MessageLabs Intelligence: 2009 Annual Security Report*, MessageLabs, available at http://www.messagelabs.com/mlireport/2009MLIAnnualReport_Final_PrintResolution.pdf.

⁶ See *MessageLabs Intelligence Special Report: Spam rates in the United States September 2009*, MessageLabs, available at http://www.messagelabs.com/mlireport/MLI_2009Sep_Spam_US_FINAL.pdf.

⁷ See <http://www.spamhaus.org/>.

⁸ See *When SPAM really is SPAM: Helping Consumers Fight SPAM*, Glass, Brett, presentation at Touro College, Jacob D. Fuchsberg Law Center, November 2007; slides available at <http://www.brettglass.com/Touro/index.html>.

those which rarely if ever have “false positive” results – but must also avoid being listed in those blacklists themselves so that their customers’ legitimate e-mail gets through. Unfortunately, due to the high prevalence of security vulnerabilities in operating systems such as Microsoft Windows, the odds are that even a small ISP with 100 customers has at least one or two “spambots” on its network at any time.⁹ For this reason, it is an industry best practice for ISPs to block unauthenticated direct outgoing e-mail transactions from customers’ computers. (These transmissions normally use TCP Port 25 and the SMTP protocol.) Some ISPs do not block such transactions altogether, but rather redirect outgoing mail to transparent proxies which watch for large flows of outgoing messages or for messages which have the characteristics of spam. This approach is problematic, however, in that a “spambot” may be able to transmit sufficient spam to cause a nuisance, and/or have the provider blacklisted, before the proxy recognizes it. Therefore, ISPs are increasingly insisting that senders of e-mail to servers beyond the boundaries of their networks use either a local mail server or some form of authenticated mail transmission.

4. BLOCKING OF MALICIOUS E-MAIL ATTACHMENTS

Many users’ computers are infected in the first place, and become “zombies,” because the user unwittingly opens an e-mail attachment containing malicious software. Many ISPs, including LARIAT, therefore employ various means to recognize and block attachments that may be malicious. LARIAT, because it implemented this practice earlier than most ISPs, was one of the relatively few which successfully and completely blocked the “Melissa” worm. Not a single copy of the worm was able to traverse LARIAT’s e-mail system, which was on the lookout for Microsoft Office documents with potentially malicious macros.

⁹ See *F-Secure IT Security Threat Summary for the Second Half of 2008*, available at http://www.f-secure.com/en_EMEA/security/security-lab/latest-threats/security-threat-summaries/2008-4.html.

5. CONCERNS REGARDING THE PROPOSED RULES

Unfortunately, even though all of the measures LARIAT takes to fight spam and malicious software are generally considered to be “best practices” in the industry and are much appreciated by our users, some of them might run afoul of the rules proposed in the NPRM. In particular, some of the participants listed in the Notice of Ex Parte Communication, while not having experience as Internet service providers themselves, have advocated strongly and publicly for rules which would preclude all of the practices enumerated above as well as others in which LARIAT may engage for the benefit of its users.

Several commenters in this proceeding have already voiced concerns that the very prescriptive rules as proposed may exceed the Commission’s statutory authority,¹⁰ which in turn may or may not be fully delineated by the Court in Comcast’s recent challenge to the Comcast Order.¹¹ Therefore, to avoid potential long term confusion in the industry, as well as discouragement of investment and other deleterious effects, Commission should instead draft simpler rules which promote competition, prohibit anticompetitive behavior, and require sufficient transparency to enable consumer choice. LARIAT’s customers have been especially vocal when they have observed even the smallest problem with regard to management of our network, and – like customers of any ISP – would surely vote with their feet if they felt that we, in any way whatsoever, made the Internet less “open.”

Respectfully submitted,

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

¹⁰ See, e.g., Center for Democracy and Technology January 14, 2010 Comments, GN Docket No. 09-191 and WC Docket No. 07-52 at 11-22; CompTIA January 14, 2010 Comments, GN Docket No. 09-191 and WC Docket No. 07-52 at 7-10; Barbara S. Esbin January 14, 2010 Comments, GN Docket No. 09-191 and WC Docket No. 07-52; Comcast January 14, 2010 Comments, GN Docket No. 09-191 and WC Docket No. 07-52 at 22-26.

¹¹ See *Comcast Corporation v. FCC*, No. 08-1291 (D.C. Cir. Sept. 4, 2008).