Seven Network Neutrality Principles and Guidelines for Appropriate Regulation

by Brett Glass
LARIAT.NET
brett@lariat.net

1. Access. All Internet users should have access to the legal content of their choice. However, it is unreasonable for them to expect to obtain this content at infinite speed, or via protocols or programs that disrupt or monopolize the network or violate the terms of service to which the user has agreed. Peer-to-peer (P2P) file “sharing” protocols and software often do disrupt and attempt to monopolize networks, and violate most ISPs’ terms of service. Content providers should therefore provide alternate, non-P2P means to reach their content (as many do already). ISPs should be held blameless if the content provider chooses not to provide such alternate means of access. ISPs should also be held blameless if they block traffic so as to halt abuse. Likewise, ISPs should be entitled to block traffic to and from networks that control networks of commandeered machines ("botnets"), host malicious software or spyware, or serve as collection points for personal data harvested from users' machines by malicious software or via users' Web browsers.

2. Disclosure. All Internet users are entitled to full disclosure of ISPs' terms of service and general network management policies, and how they apply to different service offerings from that ISP. Such disclosure should include such information as permitted and forbidden activities (e.g. whether operation of servers is permitted), as well as whether these are allowed under different service plans. (For example, P2P or operation of servers might be allowed under measured plans but not under "flat rate" plans.) ISPs shall be entitled to offer different levels of service, including service plans with differing throughput caps and pooled or unpooled backbone capacity. For plans that guarantee a minimum throughput to the ISP's backbone connection or a minimum latency, the ISP should provide or recommend a means of measurement to ensure that it is fulfilling its obligation to the user. However, ISPs should not be required to disclose technical details that might allow hackers to bypass security measures, or which would have to be tediously updated minute-by-minute as new security risks (such as worms or software vulnerabilities) surfaced.

3. Communication with customers. Internet service providers should, after proper disclosure, be allowed to communicate with customers via mechanisms which temporarily redirect or modify the behavior of the user's Web browser (e.g. by redirecting it to a "splash page," framing pages, or including a message above the page requested by the user). If the message is not a notification that service has been discontinued, the user should be allowed to opt out of repeated displays of the message once it has been received and understood.

4. Anticompetitive conduct. Internet service providers should be prohibited from engaging in practices that are directly anticompetitive. For example, a telephone company should not be allowed to block or degrade the services of third party voice over IP (VoIP) providers, nor should a cable company be allowed to hinder the receipt of video programming via the Internet. Likewise, a telephone company or other "first tier" provider should not be allowed to price

wholesale services (e.g. Internet backbone bandwidth delivered via leased lines, or the price of leased lines to a third party backbone provider) so as to drive a second tier provider's wholesale costs above retail, nor should it be allowed to refuse to deal with providers which wish to buy wholesale services from it.

5. Disclosure of behavior of client software. Content providers and third party service providers should be required to disclose *prominently* to potential users whether their software is capable of turning the user's machine into a server, or whether it consumes any resources (e.g. CPU time or network bandwidth) beyond what is required to transfer content or provide service to that individual user. Content and service providers should also turn off, by default, any features that cause the user's machine to become a server, and only allow such features to be turned on if the user chooses to enable them and the ISP indicates (via an electronic query mechanism such as the "wpad.dat" file commonly used to set caching parameters) that such use is permissible. Note that this mechanism should be consulted regularly and upon establishment of a new network connection, since the computer may be moved from network to network and permissible activities may vary by service plan or by venue. (For example, a public Wi-Fi hotspot might be more heavily restricted than a private connection.)

6) No obfuscation. Just as Internet providers should be required to disclose their terms of service and network management policies, implementors of software — in particular P2P software — should not attempt to obfuscate the presence or use of their products. While the content may be encrypted for security or privacy purposes, the fact that a particular activity — e.g. P2P — is taking place should not be obscured, so as to facilitate proper prioritization of traffic and bandwidth management.

7. Right to halt abuse. Notwithstanding any other rules that may be promulgated or adopted, ISPs must retain the right to halt abuse of their networks and to enforce their acceptable use policies and terms of service. Any rule which might have "chilling" effects on network maintenance or management could, potentially, lead to interruption or severe degradation of broadband service -- which, as consumers and businesses increasingly rely upon the network, could in turn lead to damaging or even life threatening consequences.

Note: This is an evolving document. The latest version can be found at

http://www.brettglass.com/principles.pdf

This version is Version 1.1, dated 11 March, 2008