OPENING STATEMENT OF DR. DAVID P. REED

Adj. Professor, MIT Media Laboratory

MIT Communications Futures Program

Federal Communications Commission

25 February 2008

Harvard Law School

Good afternoon Mr. Chairman and Commissioners. Thank you for the opportunity to address you on network management by high-speed Internet Access Providers.

A brief summary of my main points is in order here.

First, providing Internet Access implies adherence to a set of standard technical protocols and technical practices that are essential for the world-wide Internet to work for all its users.

Second, variances from those standard protocols and practices damages the Internet as a whole, and all of its users.

Third, there are standard, industry-accepted processes for resolving problems that come up as the Internet evolves, including disclosure of measurement data, discussion and joint definition of new protocols, etc.

Because of these points, Comcast's secretive attempt to apply non-standard management practices creates serious problems. Survival of the Internet requires that Internet Access Providers continue to take a proper, transparent role as participants in the Internet. While I would like to see that happen without regulation, Comcast's deception of its own customers in this matter suggests to me a need for stronger intervention that will discourage such Internet Access Providers *with exclusive franchises* from the temptation to degrade the Internet by selectively damaging their customers' ability to use the full capabilities of the Internet.

Internet Access Providers do *not* create the Internet for their customers, instead they provide *access* to a larger collective system, of which they are a small part.

The Internet itself is the “network of networks” that results from voluntary interoperability among a wide variety of Autonomous Systems – networks that are not owned by each other, and which do not even have contractual obligations to each other in most cases. All it takes to be part of the Internet as an Autonomous System is to agree to participate according to the very simple ground rules of the Internet.[1] These ground rules are directly responsible for the remarkable growth, scalability, and resilient evolution of the Internet itself, and more importantly the growth of the Internet's utility

[1] The core ground rules were laid out in the original design begun in 1975 by Vint Cerf and Bob Kahn. On this panel, Dr. Clark and I each participated in the original development of, and have written extensively about, these Internet ground rules.

as a backbone of commerce, information exchange, and cultural growth.

The fundamental agreement among Autonomous Systems is that they collectively provide each *host*, that is each computer that is connected to any of the many Autonomous Systems, the ability to send and receive small messages called Internet datagrams to any of the other hosts on any Autonomous System in the Internet. I avoid defining a whole collection of technical terms by suggesting that you view these Internet datagrams as *envelopes* containing messages from one host to another on the Internet. The envelope is stamped on the outside with *only* four things: an address, a return address, a protocol identifier, and some marks that indicate how the message is handled as it is carried through the network. The content of each message is held “inside the envelope.” This content is meaningful only to the sending and receiving hosts.

Each Autonomous System must agree to provide “best efforts” delivery of these envelopes without reading or changing their contents – that is, a sender posts an envelope with its return address and a specified destination address, and it expects that the envelope will be routed through the network and delivered eventually to the specified address. When congestion becomes extreme in some AS, it is normal to discard messages. This is OK because the sender keeps a copy of each message. The sender resends that message in a new envelope until it is eventually acknowledged by the addressee.

Since the beginning of the Internet's design, its designers have focused on managing congestion that may arise in Autonomous Systems. From the beginning, it has been clear that the ultimate solution of the congestion problem requires that the senders causing the congestion must “slow down” their rate of sending and prioritize their traffic if need be. The network itself cannot eliminate congestion – solving the problem requires cooperation from the senders.

These congestion control techniques can only work well if they are standardized across the *entire Internet*. New techniques are introduced carefully, typically orchestrated in the Internet Engineering Task Force, which is a collection of engineers and researchers who resolve these issues Internet-wide, independent of the vendors and operators, but taking their needs seriously. Today's standard congestion control techniques involve mechanisms for detecting and notifying endpoints of congestion -- the province of the message-switching elements of the Internet -- and mechanisms to translate detections into action.

Responsibility for indicating priority and slowing down traffic is part of the standard end-to-end protocols, in particular TCP. TCP responds to such notification by rapidly slowing down its transmission. All file transfers, including BitTorrent, use TCP, so when congestion is detected, the senders slow down.

Rather than use standard congestion control mechanisms to manage congestion resulting from BitTorrent or other file transfer protocols, Comcast unilaterally and secretly deployed a two-part traffic management solution based on “Deep Packet Inspection”[2] and “RST Injection”.[3] There were a wide range of actual standards that would allow Comcast to manage and prioritize traffic, including diffserv, ECN, RED, ...[4]

Neither Deep Packet Inspection nor RST Injection are acceptable behavior by Autonomous Systems in the Internet, for a simple reason: they each violate the expectation that the contents of the envelopes are untouched inside and between Autonomous Systems. The only recorded IETF discussion I am aware of that discusses RST Injection is a paper by a respected Internet expert, Sally Floyd, which strongly rejects the notion that using RST's for congestion control is a good design.[5]

Comcast used these non-standard mechanisms in an unexpected way, potentially disrupting systems and applications that are designed assuming the expected behavior of the Internet.

A proper provider of Internet Access must use standard mechanisms. If it deems those insufficient, it is expected to bring its problems, and data that justify its needs, to the IETF, along with proposed solutions. They would then be discussed, and improvements to the standard collectively defined. This would be done openly, and without deceiving their users who expect to run standard Internet applications.

[2] Deep Packet Inspection is a technique that uses equipment to inspect the contents of the envelopes that pass through the Comcast network, matching the content in the envelopes against known patterns to attempt to figure out what the endpoints are communicating about. Companies such as Ellacoya Networks sell such gear to government intelligence agencies who need to read network traffic, and to companies who are interested in collecting network traffic statistics that require “opening the envelope” to see what is inside each message. Deep Packet Inspection is used to separate envelopes containing undesirable messages from other envelopes in the network to count them. When enough such messages are counted, another system performs RST Injection to disrupt the communications at each endpoint.

[3] RST messages are part of the TCP protocol, used by endpoints to resolve certain rare error conditions. What they mean is, roughly, “you sent me a message, but the contents were part of a conversation that no longer exists”. RST messages are supposed to be generated only by the source and destination of Internet envelopes. Heretofore, injection of RSTs in the middle of the network was primarly used by hackers to sabotage network services. Deep Packet Inspection with RST Injection is also the primary means by which the Chinese government implements Chinese policies that disrupt Internet communications among certain dissident groups.

[4] Diffserv is the Diferentiated Service standard that allows individual envelopes to be labeled with one of a standardized set of service classes – high priority, background delivery, etc. RED (Random Early Drops) is a standard method for AS's to signal congested conditions by randomly discarding packets, which has the effect of signalling the endpoints to slow down. ECN (Early Congestion Notification) is a standard method for marking envelopes that pass through congested regions of the network, so that the endpoints can decide to slow down their traffic. All of these methods have been developed by the Internet community, analyzed, simulated, and are available for use today for situations such as the congestion alluded to by Comcast in its press materials.

[5] Sally Floyd,” Inappropriate TCP Resets Considered Harmful,” Internet RFC 3360 (Aug. 2002) <http://www.ietf.org/rfc/rfc3360.txt?number=3360>

When Comcast or any Internet Access Provider claims to offer Internet Access, they implicitly agree to participate according to the standard practices of the Internet as a whole. Otherwise, all they may claim to offer their customers is “selective access to part of the Internet's capabilities”.

To sum up the problem, a franchise comes with responsibilities to meet the expectations associated with that franchise.

I would not willingly buy Internet Access that could access only the pharmacy with which the franchisee had a special deal.[6] I would not expect my Federal, State or local government to support or to sustain any government franchise to a company that deceives its customers, by interfering with standard expectations of Internet service.

[6] The implicit reference to Strowger's professed motivation for eliminating telephone “operators” by an automatic switch is intentional here. Strowger invented the automated telephone switch that bears his name because an operator employee was directing all calls seeking a funeral home service to a specific funeral home, based on a private arrangement, disadvantaging himself and other funeral home operators who were not aware of the private arrangement.