Technical and Legal Analysis of Comcast’s Network Management Practices

Satish Sunder Rajan Gopal
University of Colorado at Boulder, sunderrs@colorado.edu
Technical and Legal Analysis of Comcast’s
Network Management Practices

by

Satish Sunder Rajan Gopal
B.Tech., Pondicherry University, 2009

A thesis submitted to the
Faculty of the Graduate School of the
University of Colorado in partial fulfillment
of the requirement for the degree of
Master of Science

Department of Interdisciplinary Telecommunications
2011
This thesis entitled:
Technical and Legal Analysis of Comcast’s Network Management Practices
written by Satish Sunder Rajan Gopal
has been approved for the Interdisciplinary Telecommunication Program

________________________________________
Paul Ohm

________________________________________
Dale Hatfield

________________________________________
Preston Padden

Date ________________

The final copy of this thesis has been examined by the signatories, and we
Find that both the content and the form meet acceptable presentation standards
Of scholarly work in the above mentioned discipline.
Comcast took a controversial decision by targeting P2P (peer to peer) specific protocols to control congestion in upstream traffic over its network. In 2008, FCC required Comcast to stop and reveal details of their current network management practices that violated Network Neutrality obligations. Many concluded that Comcast’s actions were against Internet Engineering Task Force (IETF) standard. However, rules of network neutrality, a policy statement architected by FCC cannot be enforced. And IETF, a standards body does not control Comcast’s actions. This research focuses on a hypothetical infringement suit which shows how an internet service provider could be liable for infringement, when it deviates from IETF’s protocol standards and while controlling copyrighted material over its network. Due to a lack of clarity on standard violations with no legal implications, Title –II of Digital Millennium Copyright Act (DMCA) or Safe Harbor laws are devised, defining the role and activities of a service provider. This law seems to be a solution to help resolve conflicts between copyright owners and service providers.
Acknowledgements:

A thesis involving legal analysis of technology is not my style of doing research. But, I thank Paul Ohm for allowing me to audit his copyright law class that changed my perception of law and technology, without which I would have never decided to do a thesis. I had to bother Paul every week for simple reasons, but he was patient and helped me get past every hurdle. I thank Preston Padden for showing me the path and approach to shape my research during initial phases. I specially thank Dale Hatfield, Brad Bernthal and Bryan Tramont who completely changed my perception that law, policy, economics, business and technology have a proportional role to play. Finally the two people who supported me emotionally and gave me confidence and the opportunity to succeed are Frank Stephenson Barnes and Timothy X Brown. I can never forget them for the rest of my life. I owe them so much that cannot be explained in words.
FIGURES

Figure

1. Sandvine PTS serving one CMTS .......................................................... 6
2. Session Identification ........................................................................... 7
3. Managed Protocols .............................................................................. 9
4. Protocol Agnostic Practice ................................................................. 11
5. Upstream Congestion Determination .................................................... 12
6. QoS change from BE to PBE ............................................................... 14
7. Server QoS Management .................................................................... 14
8. TCP Header .......................................................................................... 16
9. TCP Information Flow .......................................................................... 17
10. Three-way Handshake ......................................................................... 17
11. TCP Connection Establishment ........................................................... 18
12. Use of TCP Reset ............................................................................... 20
Internet is a self-sustaining disruptive innovation, meaning it has the ability to create new business models (and eventually new markets) that can compete with existing and already successful brick and mortar models thereby changing technological adoption trends. An excellent example is the growth in video on demand and rental video services between Netflix and Blockbuster®. According to Megan O'Neill (2011) a revenue analysis between Netflix and Blockbuster® from 2004 to 2010 shows that Blockbuster® has been bankrupt due to innovation in online video on demand services offered by Netflix. Utilizing the potential of convergence, it is fair to conclude that there is a tremendous economic value involved for the micro and macro scale markets in using internet as a medium.

Barbara van Schewick (2010) describes in her book, “Internet Architecture and Innovation” about the origin of internet as an experiment which initiated through a funded project by the Department of Defense (DOD) to create a network for communications, and today has integrated telecommunications globally combining voice, video and data services.

During the decade between 1980 and 1990 there were concerns on who owned the internet? In the book, “Who controls the Internet? Illusions of a Borderless World” by Jack Goldsmith and Tim Wu (2006), they explain in detail how John Postel and Vinton Cerf were responsible in maintaining the internet’s Domain Naming System (DNS) under a contract agreement with the U.S. government. The government later decided to outsource the domain naming system because they had realized that the growth of internet could be used in enhancing the nation’s economy. Following this action by the government, there was retaliation from the founders of internet, Vinton Cerf, John Postel and a group of engineers to keep the control of internet away from the
government by creating a standards body called the Internet Engineering Task Force (IETF) in 1986. Over 40 years have passed since the inception of internet, but this incident is of particular importance because it marks the beginning of what we question today, “Should internet be regulated and controlled as opposed to being an open uncontrolled domain?”

Owing and control of Copyrights, Patents and in general Intellectual Properties (IP) are crucial for a firm’s dominance in a particular relevant market (Diana Moss, personal communication, 3rd March 2011). *A&M Records, Inc. v. Napster, Inc.* marks a revolutionary copyright infringement law suit. Due to growth in, “peer-to-peer” or P2P technology and availability of music albums in a digital format online, internet users could use P2P software to download copyrighted materials for free thereby violating rights under 17 USC §106, which are the exclusive rights of copyright owners. This suit marks the second landmark historical event on the argument of control over internet.

The debate in question, from this papers perspective is the role of an online service provider like Comcast, Century Link etc. and their involvement with copyright owners. DMCA is an important piece of legislation crafted by congress to protect the market[s] created by internet and service providers. It also addresses another crucial parallel regarding the role and the activities of a service provider.

The development of DMCA is comparable to the periodic classification of elements. During the initial decade of 20th century, scientists’ would discover elements and based on its physical and chemical attributes, they placed it respectively in the periodic table. However, there were gaps left between elements which were discovered with an assumption that elements matching certain physical and chemical properties for a respective block would be discovered in future and be
placed. Similarly, title-II of DMCA needs to be architected with better legal clarity on internet standard violations. Congress has taken an approach where it looks to have allowed the marketplace in figuring out gaps in §512 as law is unable to keep pace with evolution in technology.

This paper attempts to answer the following question:

Are the network management practices adopted by Comcast and their MoU agreement with content creators, consistent with the obligations under Safe Harbor Laws or § 512 of Copyright Law?

Section – I explains in detail the network management practices adopted by Comcast and the technical decisions they adopted in curbing congestion of upstream network traffic. Section – II is divided into two parts, the first part talks about technical arguments describing the fundamental use of TCP (Transmission Control Protocol) and Internet Engineering Task Force’s (IETF) standards on the restricted use of TCP Reset’s that was violated by Comcast based on their network management practices. The second part studies the legal analysis of Comcast’s congestion control management and their alliance with content creators and music industry in forming the Center of Copyright Information (CCI) to check, if such an alliance formed to educate users on copyright, violates § 512. It will be shown that Comcast does not violate § 512 while managing P2P protocols and the use of reset packets does not compromise their status as a service provider under safe harbor law. After stating this conclusion, a hypothetical law suit will illustrate how a service provider who sends reset packets to its subscribers and decides what copyrighted material can be sent over its network, is susceptible to loose protection provided by safe harbor laws. RTC v. Netcom is highlighted as an important case explaining the significance
of providing safe harbor protection for Online Service Provider’s (OSP). Several shortcomings in
Section 512, where there is lack in legal clarity on specifics of technological measures that is
needed to be considered in a consensus based adoption between copyright owners and service
providers, definition of “material” if it refers to an Internet Protocol (IP) as a whole are discussed
in Section – III titled areas requiring further studies.
Chapter –II

Network Management Practices

Network Management Practice -I

This section explains Comcast’s congestion management system on its High Speed Internet (HSI) network based on the documents submitted to FCC. This HSI service is provided on the basis of a shared network, which means that upstream and downstream bandwidth are shared amongst users in a neighborhood. Comcast claims that it experienced high-volume of bandwidth consumption mainly due to use of peer-to-peer (“P2P”) protocols like BitTorrent, Gnutella etc. and hence decided to manage P2P protocols.

The HSI network consists the following:

a) Cable Modem (CM)
   Located at the subscribers residence with a designated IP address

b) Optical Node
   Connected to CM through a hybrid coaxial cable and the CMTS

c) Cable Modem Termination Service (CMTS) (or) Data Node
   Is essentially a router that communicates with the Hybrid Fiber Coaxial (HFC) Network within a headend Community Antenna Television (CATV) facility (Cisco, 2011). Major functionality of CMTS is to handle traffic coming in and out of its ports (upstream and downstream).

   CMTS has dedicated upstream and downstream “ports” that handles traffic flow coming in and out of CMTS. Each Comcast HSI subscribers’ modem is connected to the CMTS ports. Technically a downstream port means when CMTS sends information to a subscriber of cable modem and a downstream port is active when CMTS receives information from cable modems.
Congestion Problem

Comcast identified congestion problem mainly in upstream traffic and that it was increasing rapidly. The DOCSIS 2.0 cables used was designed such that more bandwidth was dedicated to downstream traffic as opposed to upstream traffic.

In 2005 Comcast used switches by Sandvine, Inc. to counter congestion problems in upstream traffic. This was achieved by Sandvine’s ability to identify protocols responsible for generating high volume of traffic and thereby causing congestion in CMTS ports. Hence, Comcast decided that P2P protocols are the cause on congestion in upstream traffic and decided to manage those protocols only. The Sandvine device used was the Sandvine Policy Traffic Switch 8210 or Sandvine PTS 8210 to improve the Quality of Experience (QoE) (Sandvine, 2010).

Network Configuration

Comcast claims it achieved wide scale deployment of Sandvine PTS 8210 in 2007 and these devices were placed “out-of-line” so as to avoid “point-of-failures” in the network (Comcast, 2008, p.5).

![Figure: 1 Sandvine PTS serving one CMTS (source: Comcast)](image)
Devices are placed “out of line” to prevent hindrance in regular traffic flow. Upstream traffic from CMTS originating from subscribers cable modems are mirrored to the Sandvine device configured with a congestion management policy to identify protocols causing congestion in upstream traffic. Comcast claims their CMTSes has 275 cable modems sharing a single downstream port and 100 cable modems sharing an upstream port (Comcast, 2008, p.5).

Unidirectional and Bidirectional uploads

Unidirectional uploads are sessions where a subscriber only uploads information on internet. Bidirectional uploads as opposed to unidirectional uploads are sessions where a subscriber is uploading and downloading information in a “single TCP flow” (Comcast, 2008, p.7).

According to Comcast protocols like BitTorrent and eDonkey use bidirectional upload sessions, while other protocols like Ares, FastTrack and Gnutella use unidirectional upload sessions. Comcast declares that all the above protocols are being managed by Sandvine devices on their network. However, Comcast declare that they do not manage bidirectional upload sessions.

![Figure: 2 Session Identification (source: Comcast)](image-url)
The Sandvine switch uses Session Identification technique and checks for header information from layer 3, 4 and 7 in packets to identify the protocol. However, the content or payload of the packet containing music, video, picture etc. is not examined or read by Sandvine in determining the protocol type.

Section –IV will point out certain aspects of privacy based on service providers sniffing for information from layers 4 to 7 in the OSI model.

Session Identification

The managed P2P protocols are continuously monitored by Sandvine PTS through mirroring the traffic from CMTS. Session thresholds are placed on each of the above managed protocols “for equality of fair access” between each of the protocols (Comcast, 2008, p.8).

The term quality of fair access was explained by Comcast from the following example:

BitTorrent and eDonkey applications primarily use both Bidirectional and Unidirectional uploads. However, BitTorrent promotes more bidirectional uploads compared to eDonkey. When both these protocols consume the same number of total sessions, it is found that BitTorrent has higher percentage of bidirectional sessions compared to eDonkey or BitTorrent uses more bandwidth from the same number of total sessions between itself and eDonkey. This means that bandwidth consumption per session by each protocol highly differs. The following protocols observed by Comcast show the ratio of unidirectional to bidirectional traffic and upload session thresholds amongst the five managed protocols.
TCP packets flagged with RST or reset are issued by Sandvine PTS when unidirectional upload sessions initiated by the managed protocols for a particular Sandvine PTS reach a pre-determined threshold. Comcast state that, “The “reset” is a flag in the packet header used to communicate an error condition in communication between two computers on the Internet”. Uploads for a particular managed protocol is allowed to continue their sessions when they fall below the pre-determined threshold limit (Comcast, 2008, p.10).

Comcast declared it terminated these protocol specific network management practices implemented as a congestion management practice by end of year 2008.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Ratio Bi:Uni</th>
<th>Session Equivalence</th>
<th>Uni Threshold</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ares</td>
<td>(N/A)</td>
<td>150</td>
<td>150</td>
<td>Many overhead flows exist for signaling, using little or no bandwidth. The session limit is set higher to account for this. Ares is typically used for small files.</td>
</tr>
<tr>
<td>BitTorrent</td>
<td>~20:1</td>
<td>~160</td>
<td>8</td>
<td>High ratio of bidirectional to unidirectional flows. The bidirectional to unidirectional ratio varies. Typically used for large files.</td>
</tr>
<tr>
<td>eDonkey</td>
<td>~3:1</td>
<td>~42</td>
<td>32</td>
<td>Low ratio of bidirectional to unidirectional flows. Used for large files.</td>
</tr>
<tr>
<td>FastTrack</td>
<td>(N/A)</td>
<td>24</td>
<td>24</td>
<td>Typically used for large files.</td>
</tr>
<tr>
<td>Gnutella</td>
<td>(N/A)</td>
<td>80</td>
<td>80</td>
<td>Typically used for small files.</td>
</tr>
</tbody>
</table>

Figure: 3 Managed Protocols (source: Comcast)
Network Management Practice - II

Comcast claims that this is a protocol agnostic network management practice. Instead of placing demanding traffic load on network resources by certain protocols, individuals’ traffic will be managed at times when their use of bandwidth (upstream or downstream) begins to congest the network and in turn affects the neighboring subscribers’ internet experience.

Network Elements and Configuration

The HSI network consists the following:

a) Cable Modem (CM)
   Located at the subscribers residence with a designated IP address

b) Optical Node
   Connected to CM through a hybrid coaxial cable and the CMTS

c) Cable Modem Termination Service (CMTS) (or) Data node
   Is essentially a router that communicates with the Hybrid Fiber Coaxial (HFC) Network within a headend Community Antenna Television (CATV) facility (Cisco, 2011). Major functionality of CMTS is to handle traffic coming in and out of its ports (upstream and downstream)

d) Local Market Router

e) Regional Network Router (RNR)

f) Traffic Management Servers:
   i) Internet Protocol Detail Record Server (IPDR)
      It collects CM usage statistics such as aggregate upstream and downstream bytes used by subscribers over a time period.
   ii) Congestion Management Fairshare Server (CMF)
It is otherwise called a Sandvine Congestion Management Fairshare server. It collects CMTS port utilization data using Simple Network Management Protocol (SNMP).

iii) Packet Cable Multimedia Server (PCMM)

This server is responsible in implementing Quality of Service (QoS) by changing the traffic state of individual cable modems by signaling the CMTS.

g) Internet Backbone Router

![Figure: 4 Protocol Agnostic Practice (source: Comcast)](image)

Traffic Degradation mechanism

Traffic Degradation or QoS levels are classified into two categories:

a) Priority Best Effort Traffic (PBE) set as default.

b) Best Effort Traffic (BE)
Comcast degrades a subscriber’s internet experience from PBE to BE only when the following conditions are met:

Near Congestion State

CMTS handles traffic coming in (upstream traffic) and out (downstream traffic) of its ports from the cable modems of individual subscribers. Two parameters are used to determine this congestion state in CMTS ports; Port Utilization Threshold measured in percentage of aggregate upstream or downstream bandwidth respectively and Port Utilization Duration measured in minutes. Thresholds set for downstream Port Utilization Threshold is 80% and upstream Port Utilization Threshold is 70% for a 15 minute Port Utilization Duration (Comcast, 2008, p.7).

![Image of the flow chart](source: Comcast)

The flow chart describes when an upstream CMTS port has been congested. If congestion occurs by checking Port Utilization Threshold, the system determines that Near Congestion State might
occur and then checks for Port Utilization Duration. The CMF server measures traffic at CMTS ports to detect Near Congestion State.

Extended High Consumption State

If a subscriber has been identified (mainly through his IP address from the DHCP server) to consume an average of greater than 70% bandwidth, then his/her traffic state is changed from PBE to BE. This is called Extended High Consumption State (Comcast, 2008, p.9).

During Extended High Consumption State, CMF server queries for cable modem data (IP addresses) from IPDR server. Finally, CMF server signals the PCMM servers to set new QoS policy or traffic degradation on the subscriber. PCMM server in turn sets the new QoS on the CMTS to change state from PBE to BE. BE traffic is a state when degradation of internet services is experienced during peak congestion periods. The subscribers packets in this state are given lower priority are made to wait in a queue only ensuring best effort delivery of IP packets. Comcast claims that the major advantage in this system is the traffic of the subscriber who utilizes more than his provisioned upstream bandwidth is managed. A subscribers traffic status is changed from BE to PBE, when the bandwidth consumption falls below 50% of provisioned bandwidth for a 15 minute Port Utilization Duration.

Figure: 6 QoS change from BE to PBE (source: Comcast)
Similarly, the CMF server determines the drop in upstream traffic of the subscriber, it instructs PCMM to revert to the default QoS policy on CMTS for the particular subscriber.

The following chart explains how network traffic transitions from PBE to BE state. IPDR server collecting all modem usage statistics reports from CMTS. CMF server collects port utilization statistics from CMTS using SNMP, while querying IPDR server for selected usage bytes. Based on the usage levels, the CMF server instructs the PCMM or QoS server to change traffic priority.

Figure: 7 Server QoS Management (source: Comcast)
Chapter- II

Technical and Legal Analysis

Section-I explains the network management practices adopted by Comcast based on a common theme, “degradation of internet experience” when subscribers cross a pre-determined threshold limit. This section will highlight both technical and legal arguments based on the means adopted by Comcast in achieving their ends of mitigating congestion by degrading internet experience. Technical arguments are made from IETF’s (Internet Engineering task force) RFC (Request for Comments) memorandum. Legal arguments are made from statutes in title 17 USC Section 512 or Section 512 of Copyright Law which is otherwise termed as Safe Harbor Laws for Online Service Providers. This section will attempt to answer the first part of the research question which is, “Are the network management practices adopted by Comcast consistent with Safe Harbor Laws?”

Transmission Control Protocol (TCP)

It is important to understand the following fundamentals of Transmission Control Protocol (TCP) before beginning the technical argument.

TCP Header format

“The Transmission Control Protocol (TCP) is intended for use as a highly reliable host-to-host protocol between hosts in packet-switched computer communication networks, and in interconnected systems of such networks” (Defense Advanced Research Projects Agency [DARPA], 1983, p.1).
This is the format of a TCP header and few of the fields in TCP header are explained below, due to scope of the research question. The source and destination ports along with source and destination IP addresses identify a TCP connection between two hosts. The Sequence number field contains the sequence number allotted when the first data byte is carried out in a segment. The Acknowledgement field has information on the data flow for the respective direction. The Flag field relays control information among TCP peers (Peterson et.al, 2007, p.389). The six bit Flag options available for a TCP connection are:

a) SYN – to establish a TCP connection
b) ACK – validating the Acknowledgement field
c) RESET – is discussed in detail later
d) PUSH – notification of receiving
e) URG – packet/packets containing urgent data
f) FIN – to end a TCP connection
TCP uses Segment Format and Sliding Window Algorithm

It is important to know how the information flows in a TCP connection. As a byte-oriented protocol, TCP on the sender side buffers bytes into a packet and sends these packets to receiver. The receiver reads these packets received by buffering out information. The packets which are sent and received in a TCP connection are called segments (Peterson et.al, 2007, p.388).

Three-way Handshake

Three-way handshake is an algorithm used by TCP to establish a connection between two hosts using TCP.

1) A --&gt; B SYN my sequence number is X
2) A &lt;-- B ACK your sequence number is X
3) A &lt;-- B SYN my sequence number is Y
4) A --&gt; B ACK your sequence number is Y

Figure: 10 Three-way Handshake (source: DARPA)

If A and B are two peers/hosts on internet and when host A wants to establish a TCP connection with host B, the sequence number of A must be sent to B. B in turn must confirm an acknowledgement of initial sequence number to A and also notify A regarding its (B’s) sequence
number. Following this A notifies an acknowledgement on/off the sequence number sent by B. It should be noted that steps 2 and 3 “are combined in a single message” (DARPA, 1983, p.27).

This is a basic understanding on how a TCP connection is established; the following example will illustrate an accurate description on how connection synchronization is established in a three way handshake:

<table>
<thead>
<tr>
<th>TCP A</th>
<th>TCP B</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. CLOSED</td>
<td>LISTEN</td>
</tr>
<tr>
<td>2. SYN-SENT</td>
<td>&lt;SEQ=100&gt;&lt;CTL=SYN&gt;</td>
</tr>
<tr>
<td>3. ESTABLISHED</td>
<td>&lt;SEQ=300&gt;&lt;ACK=101&gt;&lt;CTL=SYN,ACK&gt;</td>
</tr>
<tr>
<td>4. ESTABLISHED</td>
<td>&lt;SEQ=101&gt;&lt;ACK=301&gt;&lt;CTL=ACK&gt;</td>
</tr>
<tr>
<td>5. ESTABLISHED</td>
<td>&lt;SEQ=101&gt;&lt;ACK=301&gt;&lt;CTL=ACK&gt;&lt;DATA&gt;</td>
</tr>
</tbody>
</table>

Figure: 11 TCP Connection Establishment (source: DARPA)

Here TCP A initially being closed, attempts to establish a connection with TCP B as shown in step 2. It sends a SYN segment with Sequence number 100 and CTL is a 6 bit FLAG field in TCP packet set to SYN. In step 3, TCP B on receiving this segment sends another segment with a sequence number followed by a SYN and ACK response to segment sent by TCP A. In step 4, TCP A sends a segment with sequence number containing ACK of TCP B from the previous step. This step marks the establishment and synchronization of connection and data is eventually sent during step 5.

Now that, the fundamentals of TCP are illustrated, following parts will focus on technical and legal arguments based on network management practices and congestion control mechanism adopted by Comcast in curbing upstream traffic.
Technical Arguments: Understanding IETF’s Priority RFC Documents

“The IETF is the protocol engineering and development arm of the Internet” (IETF). It was formally established by Internet Architecture Board (IAB) in 1986. IETF are group of engineers working in developing standards for internet protocols. It is to be noted that IETF is not involved in standardizing hardware involved in transmission at layer 1 and layer 2 of OSI/OSI and certain application layer standards like Hyper Text Transfer Protocol (HTTP) and Exchange Markup Language (XML). But IETF does standardize all protocols from layer 3 to application layer 7. IETF produces official documents called Request for Comments (RFC) which gives technical descriptions on new standards developments. However, IETF asserts that, “not all RFC’s are standards. Only RFCs that open with words like "This document specifies an Internet standards track protocol" or "This memo documents an Internet Best Current Practice" are normative documents approved by the IETF (Most recently, they will also have a header stating "Category: Standards Track" or "Category: Best Current Practice")” (IETF, 2011).

RFC standards are formally recognized in order of their official stages of importance:

a) Proposed Standard (PS) – Normative Document
b) Draft Standard (DS)
c) Standard (STD)
d) Best Current Practice (BCP)- Normative Document

TCP Reset (or) TCP_RST

RFC 793 defines the significance of TCP RST bit as, “The principle reason for the three-way handshake is to prevent old duplicate connection initiations from causing confusion. To deal with this, a special control message, reset, has been devised” (DARPA, 1983, p.31).
An example of confusion relating duplicate connection is as follows:

<table>
<thead>
<tr>
<th>TCP A</th>
<th>TCP B</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.  (CRASH)</td>
<td>(send 300, receive 100)</td>
<td></td>
</tr>
<tr>
<td>2.  CLOSED</td>
<td>ESTABLISHED</td>
<td></td>
</tr>
<tr>
<td>3.  SYN-SENT --&gt; &lt;SEQ=400&gt;&lt;CTL=SYN&gt;</td>
<td>--&gt; (?)</td>
<td></td>
</tr>
<tr>
<td>4.  (!!!)</td>
<td>&lt;-- &lt;SEQ=300&gt;&lt;ACK=100&gt;&lt;CTL=ACK&gt;</td>
<td>&lt;-- ESTABLISHED</td>
</tr>
<tr>
<td>5.  SYN-SENT --&gt; &lt;SEQ=100&gt;&lt;CTL=RST&gt;</td>
<td>--&gt; (Abort!!)</td>
<td></td>
</tr>
<tr>
<td>6.  SYN-SENT</td>
<td>CLOSED</td>
<td></td>
</tr>
<tr>
<td>7.  SYN-SENT --&gt; &lt;SEQ=400&gt;&lt;CTL=SYN&gt;</td>
<td>--&gt;</td>
<td></td>
</tr>
</tbody>
</table>

Figure: 12 Use of TCP Reset (source: DARPA)

Here, two hosts A and B using a TCP connection are exchanging information and during the process host A disconnects due a crash. Assuming that state of the art operating systems are being used, memory loss caused due to the crash is recoverable. After recovery TCP link on host A is activated and establishes synchronization with B either from beginning or from a specific recovery point. If A establishes a connection from a recovery point, B receives an error message from A. When TCP A crashes it tries to re-open the connection, while TCP B thinks that the previous connection is open. As TCP A opens the connection show in step 3 with a new SEQ number, TCP B’s state is synchronized and acknowledges the new incoming segment with the old sequence number it step 1. Receiving this segment A does not acknowledge it and sends a reset (RST) because A is in an unsynchronized site and it has detected a “half-open connection” (DARPA, 1983, p.33). In step 5 TCP B aborts the connection and TCP A synchronizes the new connection with SEQ number 300.
Analysis of TCP reset: A technical Argument

Now that the fundamentals of TCP_RST are illustrated, it is important to think about the following questions:

a) Why was Comcast’s decision on issuing TCP_RST packets in peer to peer TCP connections wrong (or) not recommended?

b) Does IETF specifically state or give a clear indication that use of TCP_RST packets as a tool for congestion control mechanism illegal or not recommendable in any of its RFC’s?

c) Is the protocol agnostic network management practice adopted by Comcast to deal with congestion in upstream traffic, consistent with IETF standards?

Why was Comcast’s decision on issuing TCP_RST packets in peer to peer TCP connections wrong (or) not recommended?

Documents were submitted by Comcast to the FCC regarding their network management practices subject to 47 CFR 1.17. Based on this evidence, FCC determined in their Order regarding the complaint lodged by Free Press and Public Knowledge that Comcast proclaimed to issue TCP_RST packets in unidirectional P2P upload sessions when users in such sessions reach a predetermined upstream bandwidth limit. As illustrated in RFC 793, reset control message was primarily designed to prevent initiations of duplicate connections using three-way handshake. It should also be understood from RFC 793 that a TCP connection is generated and terminated solely by peers, purely as an administrative function. The peers in a TCP connection technically have administrative rights over that session.
Comcast states, “the Sandvine PTS issues instructions called “reset packets” that delay unidirectional uploads for that particular P2P protocol”, in this statement technical and policy violations are observed. Firstly, issuing “reset packets” in an active TCP connection administratively generated between peers by another device namely Sandvine PTS controlled exclusively by a service provider is against the TCP standard. IETF mentions in Section 5 of RFC 793 on Reset Generation, “As a general rule, reset (RST) must be sent whenever a segment arrives which apparently is not intended for the current connection. A reset must not be sent if it is not clear that this is the case.” Here Comcast’s network is neither an administrator in a TCP connection which is generated by their subscribers and issuing TCP packets flagged with reset without consent of their subscribers who do not understand why their bandwidth is being throttled, is a violation of RFC 793. Regarding the importance of RFC 793, it is a Proposed Standard (PS) RFC- a normative document, which is considered to be a serious technical norm published by IETF. Possession of this knowledge while violating the standard is comparable to going against a norm.

Secondly, the Sandvine PTS was targeting specifically P2P protocols and in turn not allowing P2P applications to function the way they are supposed. This goes against FCC’s Internet Policy Statement or Network Neutrality rules on degrading internet applications. The Net Neutrality argument will not be further discussed as it is outside the scope of this paper.

It can be asserted that, what Comcast did is inhibitive of the way a network was designed to work by intrusively (other than being a peer) modifying normal TCP session operation.
Does IETF specifically state or give a clear indication that use of TCP_RST packets as a tool for congestion control mechanism illegal or not recommendable in any of its RFC’s?

RFC 3360 a Best Current Practice (BCP) RFC distributed in 2002 specifically recommends on congestion control methods in Section 2.3 to drop the SYN packet as it is an “effective response to congestion” instead of certain hosts sending reset packets while responding to SYN packets. With this information made available by IETF Comcast choose to manage congestion by issuing TCP_RST packets and hence going against the recommendation standards set by IETF. An expert opinion by Brett Glass concludes that the use of TCP_RST by party other than the peer of a TCP session is against the internet standard and is an action intended to harm and interfere with TCP’s functionality, confusing the users, their software (Glass, 2008).

Is the protocol agnostic network management practice adopted by Comcast to deal with congestion in upstream traffic, consistent with IETF standards?

The protocol agnostic network management practice adopted by Comcast goes in accordance with the recommendation in Section 2.3 of RFC 3360 where congestion can be dealt with by dropping SYN packets instead of using TCP headers flagged with reset. RFC 3360 recommends in Section 2.3 that dropping SYN packets is “the most effective response to congestion”, so there is no standard violation and strong evidence against Comcast as far Section 512 is concerned. The two priority statuses viz. PBE and BE are reasonable and in accordance with RFC 3360 and RFC 793. It is less disruptive to the client P2P sharing software if SYN packets are dropped because it will accordingly adapt and respond by the functionality of TCP’s sliding window algorithm; to the network bandwidth requirements. Dropping SYN packets is a normal and expected event that the TCP protocol was designed to handle. Injected reset packets by someone
other than the administrators are outside of the TCP specification and can cause unintended behavior for the clients.

Data Over Cable Service Interface Specifications (DOCSIS) is standard for cable modem which allows high speed data transfer on Cable TV (CATV) developed and certified by CableLabs (DOCSIS, n.d.). With the evolution from DOCSIS 2.0 to DOCSIS 3.0, that comes with a new feature “Channel Bonding” Comcast will be able to provide better upstream bandwidth by combining several upstream channels from HFC, collectively called a bonded group (DOCSIS, n.d.). This new feature supplemented with better upstream bandwidth management, hopefully Comcast will not revert into using TCP_RST packets as an effective technique for congestion control.

Legal Arguments

The technical section highlights how Comcast strayed away from IETF’s TCP standards; this section will attempt to co/relate legal shortcomings by Comcast and technical violations. The approach taken to achieve this co/relation is by understanding the role and responsibilities of a service provider dictated by Congress in order for online service providers (OSP) to qualify for Title-II of the Digital Millennium Copyright Act (DMCA) or added as Section 512 to the Copyright Act which is Online Copyright Infringement Limitation Act (OCILLA). As discussed earlier this act establishes safe harbor rules that provide immunity to online service providers against copyright infringement by their subscribers. However, before beginning the discussion on Section 512 violations by Comcast it is important to understand why Congress provisioned such safe harbor rules to protect online service providers. Legal analysis will later show that
Comcast does not violate § 512 based on its network management practices and its role in being a member of Center for Copyright Information (CCI).

Infringement

Infringement of a copyrighted material means, violation of the “exclusive rights” of copyright owners under Section 17 U.S.C § 106 (Cohen et al., 2006).

Understanding why Section 512 was provisioned for OSPs': Technology and Infringement

If one were to copy a copyrighted material by writing into a paper, it is an infringement against the author of that material unless the infringer has a substantial defense to his actions. However, when technology intervenes when an infringer uses it to copy a published material, it complicates the scenario by raising the question, is the manufacturer of that technological device liable for infringement for enabling copying protected material? For ex: a photocopy machine can be used to copy and print protected materials, so does that mean the author should file a suit against the infringer who printed protected material and the printer’s manufacturer who enabled the infringer to produce copies? Or speaking from this paper’s perspective, if an infringer scans the protected material and posts them on an online forum like www.overclock.net using an internet connection provided by Comcast or CenturyLink, does this mean that the author must file suit against Comcast’s or CenturyLink’s network because they carry those copies in form of packets all over internet and also hold overclock.net liable for allowing infringing materials to be posted in their forum? (Cohen et al., 2006).

These are important questions because an infringer’s actions should not be responsible in suits being filed against manufacturers’ of technology and innovation because it contradicts the very
purpose of Article I Section 8 of the United states Constitution that states, “To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries;” The term “Progress of Science” is rendered meaningless if authors’ of protected materials are allowed to file suit against manufacturers, distributors and entities offering services using technology. The following case highlights all liabilities against service providers as it marks an important landmark that lead to the addition of Section 512 into Copyright Law. This case will help understand the several liabilities faced by service providers due to infringement of material online by their subscribers at a time, when DMCA was not created.


Justice Whyte declared the findings of this case in a summary judgment (Summary Judgment under the Federal Rules of Civil Procedure, Rule 56 means a party can move towards summary judgment in they can show all “material facts” of the case that show no “genuine dispute” to the court and as a matter of law the will allow such a motion) that raised several questions on intellectual property rights in cyber space.

Religious Technology Center (RTC) and Bridge Publications, Inc. (“BPI”) are the plaintiffs holding copyrights of Lafayette Ron Hubbard. These copyrights contain both published and unpublished works.

Defendants are Dennis Elrich (“Elrich”), alt.religion.scientology (“a.r.s”) an online discussion forum on “discussion and criticism of Scientology”. Elrich accessed internet through defendant
Thomas Klemesrud’s (“Klemesrud’s”) operator of a BBS (Bulletin Broadcast Service) running from Elrich’s home with 500 paying users. Klemesrud’s BBS is connected to internet through Netcom On-Line Communications, Inc. (“Netcom”), who then was one of the largest internet providers in United States.

Issue

The case attempts to address if an online bulletin board service (BBS) and an Internet Service Provider who enables the BBS to connect to internet are liable for copyright infringement by a subscriber using both services.

Plaintiffs claim

The plaintiffs claimed Elrich’s postings infringed their copyrights by posting the materials on a.r.s.

Plaintiffs initially approached Elrich to stop the postings but failed to convince, then contacted Klemesrud and Netcom. Klemesrud then asked plaintiffs to “to prove that they owned the copyrights” of Elrich’s postings to which plaintiffs considered it as an “unreasonable” request and did not comply. Similarly Netcom refused plaintiffs request on not allowing Elrich get access to internet through their network as Netcom asserted that “to kick Elrich off the Internet meant kicking of hundreds of users of Klemesrud’s BBS”. Hence, plaintiffs name Klemesrud and Netcom as defendants alongside Elrich (Religious Technology Center v. Netcom On-Line Communication’s Services, 1995).
Facts

Before beginning the arguments of infringement per se, discussing the facts on how transmission of postings by Elrich are being carried over Netcom’s system and how are the defendants are infringing collectively is important. Elrich is a paying member of Klemesrud’s BBS, which is a Usenet newsgroup or otherwise an online discussion forum on Scientology. Elrich connects to this BBS through a telephone and modem. When Elrich posts infringing material on Usenet newsgroup a.r.s, copies of these postings are made on Usenet servers and Netcom servers, making these posting available to both Netcom and a.r.s subscribers and hence worldwide access of protected material is made available as they are downloaded on several computers. While copies are made on several servers, as an automated process, these copies are saved on Netcom and Usenet servers for certain days. But the process of copying and reproduction of infringing materials is initiated by Netcom and Klemesrud only if a subscriber like Elrich initially performs the act of posting them on Klemesrud’s BBS. Netcom’s system is designed such that, it “incidentally makes temporary copies of plaintiffs’ work”, not that it is responsible for initiating the infringement (Religious Technology Center v. Netcom On-Line Communication’s Services, 1995).

Netcom did not copy

Now that the facts are discussed, the court did not rule Netcom guilty under Direct Infringement 17 U.S.C § 501 because Netcom’s system is designed to makes copies of data transmitted across internet initiated by its subscribers, but that does not mean the users of this service can directly infringe protected material and to hold a service provider liable for direct infringement is unreasonable.
Plaintiffs’ extravagant theory

Based on plaintiffs’ theory that after Elrich’s posting, copies are made by Usenet servers across the internet without human intervention and hence every server is liable for carrying the copied material is also unreasonable.

No Intent to copy

As, there was no intent of “violation or causation”, in Netcom’s network architecture and Klemesrud’s BBS the court held that they are not liable under direct infringement. Court also points out to plaintiffs’ theory that the “damage” could have been “lessened” had Netcom complied with plaintiffs’ request is not a relevant claim under direct liability and that the concept of “knowledge” of infringement by defendants’ is irrelevant (Religious Technology Center v. Netcom On-Line Communication’s Services, 1995).

Courts holding

Hence, the court finds Netcom and Klemesrud’s BBS are not liable for directly infringement and do not violate any exclusive rights of plaintiffs’ under 17 U.S.C § 106.

However, being relived from direct infringement does not relieve Netcom on the question of secondary liability. Secondary liability rules are made by court and are not incorporated into statute. The court had to analyze from plaintiffs’ claim, if Netcom is guilty under the secondary liability test? There are two kinds of secondary liability test: Contributory Infringement test and Vicarious Liability test.
Contributory Infringement

From Gershwin Publishing Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (2d Cir. 1971), liability under contributory infringement is when a defendant, “with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another”. The important elements here are actual “knowledge” and “induced cause or materially contribute to the infringement”. These are still considered as a third party liability (Religious Technology Center v. Netcom On-Line Communication’s Services, 1995).

Netcom were approached by plaintiffs’ who notified them on the infringements made by Elrich on Klemesrud’s BBS, with this information available to defendants, plaintiffs’ claim that Netcom had the “knowledge” of infringement and refused to take action. Netcom made counter claims of not possessing any knowledge as it was unaware of Elrich’s “planned infringing activities” while leasing facilities to Klemesrud, it wasn’t aware that Elrich “would infringe prior to any of his postings”, it could not screen out Elrich’s infringing post’s, “before they were made” and finally it could not access if plaintiffs’ copyrights “were valid” and that “Elrich’s use was fair” (Religious Technology Center v. Netcom On-Line Communication’s Services, 1995).

The court addressed these counter claims by asserting that Netcom not only leased facilities to Klemesrud but also acts as a service provider by transmitting information. On the claim of not being aware of Elrich’s infringement, courts said that the “relevant time frame” of having knowledge of infringement is when Netcom continued its services after being notified by plaintiffs’ on infringement, “not when Netcom entered into an agreement with Klemesrud” (Religious Technology Center v. Netcom On-Line Communication’s Services, 1995).
Issue

The main issue on contributory infringement especially on the element of “knowledge” is if “Netcom knew of any infringement” and if “it was too late to do anything about it”. BBS operator’s inability to assess the infringement claim without “lack of copyright notices”, “possible use of fair use defense” or failure on copyright owner “to provide necessary documentation to show that there is likely an infringement” is reasonable and that there is no liability for contributory infringement for continuation of distribution of information in the system (Religious Technology Center v. Netcom On-Line Communication’s Services, 1995). Netcom admitted that it never looked at the postings after being notified by plaintiffs’ who provided “statements regarding authorship” and hence taking no action into investigating raises the question of “knowledge”. Hence, it is a fair assumption that Netcom participated in contributing towards infringement without taking measures of preventing “further damage to plaintiffs’” protected works while allowing Elrich to continue posting infringing materials is comparable to “induces, causes or materially contributes to the infringing conduct” Plaintiffs’ theory on contributory infringement raises an important question on “knowledge” of infringement and “materially contributing” or “participating” in Elrich’s infringement (Religious Technology Center v. Netcom On-Line Communication’s Services, 1995).

Vicarious liability test

Vicarious liability comes from agency law and is another secondary liability theory that plaintiffs can use when contributory test fails. Under vicarious liability, a defendant is found guilty based on the actions of primary infringer when the defendant

a) “has the right and ability to control infringers actions” and
b) “receives a direct financial benefit from the infringement”

The important elements here are “right and ability to control infringers’ actions” and “receives a direct financial benefit”. The burden of proof is on the plaintiffs’ to prove both the elements to hold defendant liable under vicarious test. Plaintiffs’ dispute the fact that under Netcom’s terms and conditions “to which its subscribers must agree” and Netcom “reserves the right to take remedial action against its subscribers” Plaintiffs’ also argue under IETF’s RFC 1855 Netiquette Guidelines that, “the access provider has a duty [to] take measures” against violation of copyrights. Plaintiff’s raise an important question on Netcom’s “right to control Elrich”. An expert opinion from plaintiffs’ side disputes the fact that Netcom could have easily identified these postings that contain specific words and the individual by a software modification. Netcom had the “right and ability to control” Elrich’s posting by deleting them where the timing of infringement in this test is not important. Hence, the court find plaintiffs’ claims genuine and that they have raised an important question on Netcom’s “ability to exercise control” over its subscribers. Thus, plaintiffs’ satisfy the first element of vicarious liability, now the burden of proof is to show “a direct financial benefit” to Netcom from the infringement (Religious Technology Center v. Netcom On-Line Communication’s Services, 1995).

The following case helps understand the significance of a direct financial liability. From Shapiro, Bernstein, 316 F.2d at 306, “a landlord having “the right and ability to supervise”, the tenant’s activities will be vicariously liable for infringement of tenant” because the rent collected by the landlord is through the supervision of tenant. When the tenant’s rental space or services operated are based on “fixed rental fee” independent of tenant’s activity, courts “usually” do not consider

In this case, looking at the financial connection between Elrich and Netcom, it can be seen that Netcom charge their subscribers (Elrich included) a fixed fee based on bandwidth and service type chosen by individual subscribers. Also, Netcom admit that they do not “create or control the content of information available to subscribers’”, comparing this with the prior example, where the owner charges a fixed rental fee and does not involve with tenant’s activities, Netcom is in the same position. Where Netcom are not involved with subscribers’ activities and don’t not gain a direct financial benefit from Elrich’s infringed postings as they charge a fixed fee, Netcom is not vicariously liable for infringement by Elrich’s posting. The court determined that plaintiffs’ failed to provide an evidence of direct financial gain by Netcom from Elrich’s infringed postings and hence fail the vicarious liability test. Roy Export, 344 F.Supp. at 1353 (Religious Technology Center v. Netcom On-Line Communication’s Services, 1995).

First Amendment and Fair Use argument

Netcom claimed a first amendment violation by plaintiffs’ liability theory that would disrupt the very functioning of internet where “every access provider or user” is liable when infringing materials are posted by users on a Usenet newsgroup. The court agreed that “an overbroad injunction” might violate the First Amendment In re Capital Cities/ABC, Inc., 918 F.2d 140, 144 (11th Cir. 1990), but liability due to infringement can apply in issues that do not raise First Amendment claims. Copyright law balances out with First Amendment claims with elements like idea/expression dichotomy and fair use doctrine, issues outside these are where
liability due to infringement applies where first amendment cannot be claimed (Religious Technology Center v. Netcom On-Line Communication’s Services, 1995).

Common Carrier Argument

Netcom claimed to act like “a common carrier” and “a passive conduit” passing information coming through it, meaning that a Usenet servers merely forwards information “like a common carrier”, by “passively retransmitting” it. Netcom’s counsel compared themselves to a “phone company” that stores “an infringing audio recording” and hence holding servers liable is comparable to holding the owner of a highway of a toll booth operator liable. But Netcom is more than a common carrier in the way its system operate and with its ability to control and monitor its system and hence cannot be placed equally as a common carrier. Also, unlike common carriers that are “natural monopolies”, internet service providers are not bound by “must carry” rules to carry all traffic. Federal Communications Commission v. Midwest Video Corp., 440 U.S. 689, 701, 99 S.Ct. 1435, 1442, 59 L.Ed.2d 692 (1979). 17 U.S.C §111 outlines rules for liability on secondary transmissions where a passive carrier is not liable for secondary transmission if it does not have “any direct or indirect control over the content of selection of the primary transmission.” 17 U.S.C. § 111(a) (3) Common carriers are hence granted certain statutory exemptions against liability and Netcom cannot be regarded as a common carrier and hence is not exempted against liability under contributory infringement (Religious Technology Center v. Netcom On-Line Communication’s Services, 1995).
Conclusion

The court concluded that plaintiffs’ fail to prove Netcom and Klemesrud’s BBS liable for Direct and Vicarious infringement but raise important facts on Contributory Infringement. Finally, the court did not rule in either party’s favor due to significant issues of contributory infringement because Judge Whyte stated that there is a “material issue” on the “knowledge element” of contributory infringement claim by plaintiffs’ (Religious Technology Center v. Netcom On-Line Communication’s Services, 1995).

Religious Technology Center v. Netcom On-Line Communication’s Services Inc. addresses crucial issues on the role of service providers and their ability to control and monitor subscribers traffic over internet. The case points out issues where service providers are susceptible to suits for secondary liability and hence forcing Congress into legislating Section 512 or Safe harbor laws. These laws assign service providers certain responsibilities in protecting copyrighted materials and uphold copyright law in cyber space, while encouraging innovation in developing computer networks to flourish by making clear legal aspects on liability for infringement in the digital world. However, from a standards perspective of networking technology there are no laws binding service providers into adopting a specific standard. While IETF sets standards on network protocols, service providers are obligated to follow them and ensure its subscribers get the best experience of internet. Straying away from IETF standards and recommendations, responsibilities assigned by Congress in safe harbor laws and confusing subscribers using TCP_RST packets in P2P upload sessions does not comply with obligations in safe harbor laws.
Due to the several claims put forth by plaintiffs’ against defendants Netcom as discussed above, the importance of DMCA’s creation to protect service providers should be realized.

Legal Analysis

§ 512. Limitations on liability relating to material online

(a) Transitory Digital Network Communications. — A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if —

(1) the transmission of the material was initiated by or at the direction of a person other than the service provider;

(2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;

(3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;

Role of service provider as a Conduit

In A&M Records, Inc. v. Napster, Inc., 54 U.S.PQ.2d 1746, 1752 (N.D. Cal. 1998), the court adopted the term “through a system” to mean a conduit. The word “conduit”, is not mentioned in § 512 and Copyright Law but is mentioned in the legislative history. Also,
according to Senate in the 105th Congress report on DMCA, § 512 (a) (1) – (5) “limit the range of activities “where a service provider “plays the role of a “conduit” ”. To understand this from a layman’s perspective, it means the responsibilities assigned to service providers like Comcast limit them to the role of a “conduit” under § 512 (a) (1) – (5) (Commerce Rep. (DMCA), 1998, p.50).

Now that § 512 (a) (1) – (5) limit the activities of a service provider to play the role of a conduit, it is reasonable to check if the network management practices adopted by Comcast before and after 2008 violates § 512 (a).

Does the network management practices adopted by Comcast violate § 512?
The technical analysis shows that Comcast violated IETF’s standard by using TCP_RST as a tool for controlling congestion. However, IETF does not monitor or bind any entity legally in following its standards. Because Comcast’s standard violation has no legal implication, the use of TCP_RST packets as a congestion control tool does not violate any part of § 512 (a).

Therefore Comcast reserve their safe harbor rights in this case. The protocol agnostic network management practice adopted after 2008, where dropping packets was used as a tool to reduce congestion in upstream traffic, is in accordance with RFC 3360. Hence, there is no IETF standard violation neither observed in this case nor is there a legal violation seen under § 512. As none of the network management practices violate § 512, the formation of Center for Copyright Information (CCI) will be looked into to check if this alliance violates § 512.
Center for Copyright Information (CCI)

In an effort to curb online-piracy, Internet Service Providers (ISP) and content creators have established an organization as a “voluntary collaboration”, called the Center for Copyright Information (CCI). CCI is designed to educate internet users the “importance of copyright protection”. This organization will develop “best-practices” in creating a “Copyright Alert” system which is similar “to credit card fraud alert” system. It attempts to help educate internet users in differentiating pirated and legitimate lawful contents (video and music) online. A MoU was agreed upon on July 6th, 2011, explains Copyright alert process in detail (Memorandum of Understanding, 2011).

The means used by CCI to educate subscribers distributing copyright material illegally using P2P software are:

a) ISP redirecting their subscribers dealing with copyright material illegally to a webpage requesting them to attend an educational program on copyright infringement

b) ISP using pop-ups in web browsers as a reminder on infringement alert.

According to this MoU, the participating ISP’s should use “commercially reasonable efforts” in sending alerts to subscribers (Memorandum of Understanding, 2011). The stages of notifications to be set up by the participating ISP’s are:

a) Initial Education Step

b) Acknowledgement Step

c) Mitigation Measures Step

d) Post Mitigation Measure Step
This section will attempt to answer the second part of the research question, “is the MoU between Comcast and content creators consistent with Section 512?”

§ 512 (i) (2): Definition — As used in this subsection, the term “standard technical measures” means technical measures that are used by copyright owners to identify or protect copyrighted works and —

(A) have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process;

This collaboration between ISP’s and content creator does not violate Section 512, because they are allowed to form such an alliance under § 512 (i) which permits copyright owners and service providers to form a broad consensus to resolve issues in online copyright infringement. In accordance to § 512 (i) (2), the service providers, content and music industry have developed a broad consensus that is open, fair, etc. which is exactly what CCI is all about. Hence, Comcast does not violate § 512 in being a member of CCI.

Conclusion

To conclude the analysis of the research question, Comcast does not violate § 512 on the counts of their network management practices and in being a member of CCI.
Chapter - III
Hypothetical infringement suit

Every action by Comcast so far is legal. What if a new alliance is formed between service providers, content creators and music industry, who implement a policy similar to Comcast by sending reset packets over their network? The following hypothetical infringement suit will illustrate how a service provider can be held liable for infringement.

Great Creations Inc. independently produces and distributes a popular low budget comedy series, “Alchemy”. It uses internet as the source to distribute its content through software from its website. It holds copyrights in all episodes of Alchemy. They use services offered by Horizon Corp. to connect to the internet whose network infrastructure was build out by a third party vendor. Horizon Corp. are an active member of the Copyright Protection Alliance (CPA) alliance formed between ISP's, content creators, Movies Association of America and Music Association of America. The members of CPA work closely in curbing piracy on internet. The content creators participating in CPA notify ISP's on subscribers download their content illegally. ISP’s then take action by educating their subscribers on infringement activity. When repeated warnings are sent to subscribers on infringement, Horizon Corp. a participating member of CPA came up with a solution to stop such repeated infringer's distributing CPA member’s copyrighted content illegally online. After consulting with several network engineers, Horizon Corp. agreed upon using Sandvine PTS 8210 which identifies BitTorrent ports generating high traffic volumes in the network. Members of CPA notify Horizon Corp. on subscribers who are identified as illegal distributors of their content online, on ISP's network. ISP’s then would take action by configuring the Sandvine switch to issue TCP_RST packets to sources of illegal traffic identified by content creators part of CPA. Great Creations Inc. observed their copyrighted content being...
pirated and distributed illegally online. Great Creation Inc. realizes their content is distributed illegally on Horizon Corp.'s network by Horizon Corp.'s subscribers who use P2P software client BitTorrent. As the CPA framework is made public, Great Creations Inc. approached Horizon Corp. and informed about the illegal content distribution and asked them to give similar treatment given to members of CPA that will stop illegal distribution. Horizon Corp. refused the claim, hence allowing the illegal distribution to continue.

Macrosoft, a software company similarly approached Horizon Corp. and requested for similar treatment as they confirmed illegal seeding of their commercial software Macrosoft Office 2012 on Horizon Corp.'s network. Horizon Corp. refused to comply.

Plaintiffs Great Creations Inc. and Macrosoft file suit against Horizon Corp. for infringement of “Alchemy” and “Macrosoft Office 2012” respectively. Horizon Corp. proclaims that it is protected by Section 512 but plaintiffs assert, Horizon Corp. violated obligations under 17 USC 512 (a) (2) and hence are no longer protected by safe harbor law.

Does Horizon Corp. satisfy the obligation under § 512 (a) (2)?
Horizon Corp.'s activities are limited to the role of a conduit and are obligated to follow rules under § 512 (a) (1) – (5) to qualify for safe harbor laws as a Transitory Digital Network (Commerce Rep. (DMCA), 1998, p.51). By issuing TCP_RST packets in a way that is against RFC 793, questions their role as a conduit. § 512 (a) (2) states “without selection of material”, which according to the legislative history means, “the editorial function of determining what material to send, or the specific sources of material to place on-line (e.g., a radio station), rather
than ‘an automatic technical process’ of responding to a command or request, such as one from a user, an Internet location tool, or another network” (Commerce Rep. (DMCA), 1998, p.51).

Horizon Corp. took an independent decision by using Sandvine PTS 8210, which mirrors traffic from CMTS and during peak congestion in upstream traffic was set to issue TCP packets flagged with reset by identifying the user’s account. Issuing TCP_RST packets by a third party other than the peers of a TCP session interferes the functioning of TCP protocol as stated in RFC 793.

Horizon Corp. is also accountable for violating Internet Advisory Board’s (IAB) RFC 1087 on Ethics and the Internet. IAB’s statement of policy identifies that “disrupting the intended use of internet” is an unacceptable and unethical activity. Disrupting TCP connections by issuing reset packets thereby confusing the administrators of a TCP session is unacceptable from the perspective of RFC 1087.

Horizon Corp. determined whose copyrighted material to send over their network. Being a member of CPA, it took immediate actions to protect copyrighted materials of CPA members by issuing TCP resets to connections illegally distributing the materials. But when approached by Great Creations Inc. and Macrosoft, it denied to take any action and allowed the illegal distribution to continue. Comparing this to Netcom case, contributory infringement clearly comes into the picture and Horizon Corp. cannot claim 512 protection, common carrier or fair use. Hence, there is no defense in this case against contributory infringement.
Conclusion

Hence, Horizon Corp. is liable for infringement (secondary liability) and they fall out of safe harbor laws.

The point that needs to be observed in this example is, service providers could be liable for infringement while making such agreements with music and movie industries and straying away from internet standards by interfering with protocols. The fact that a service provider has the authority to teach or educate an infringer and sometimes interfere with the infringers’ internet experience sounds more of a policing role. But when Section 512 (a) for example, limits the role of a service provider to that of a conduit, seems to conflict with Section (i) (1) (A) where service providers have the authority to terminate internet connections of repeat infringers.
Chapter -IV

Areas requiring further study

The Material

The word “material” has not been defined in Section 512, making it difficult to comprehend if it applies to an IP packet as a whole, wherein the fields of the packet also become a part of the material. It makes sense for Congress to intentionally leave this for the courts to decide on case by case basis. “An entity is not disqualified from being a ‘service provider' because it alters the form of the material, so long as it does not alter the content of the material” (Commerce Rep. (DMCA), 1998, p.63). Here the committee mentions, “Content of the material”, and from an engineering standpoint it can be understood that it’s being referred to the payload of a packet. But without legal clarity on the definition of material, it is difficult to come to a conclusion.

Because generating a packet with the CTL field set to RST (reset) by someone other than the users (persons as stated in § 512 (a) (1)) is against § 512 (a) (1).

Technology to fills gaps in § 512?

Leaving gaps in § 512 is reasonable from the view that technology is evolving rapidly to which law cannot keep up. But hoping that technology is the solution in filling these gaps is not reasonable because of its creative destruction nature. His develops as a policy argument. The inclusion of “standard technical measures” according to commerce report on DMCA means, “is intended to encourage appropriate technological solution to protect copyright works” (Commerce Rep. (DMCA), 1998, p.61). It means, technology is the solution that would resolve issues of copyright infringement adopted between copyright owners and ISP’s. This gives an indication
that Congress has left a gap in this statue, allowing the market place to figure out the appropriate technological measure. The important question that needs to be asked is “Are there appropriate technological measure that can be adopted to resolve issues on copyright infringement between ISP’s and content creators (or) the CCI, if so what are they?”

In CCI FAQ’s on Copyright Alert System, ““Mitigation Measures,” might include, for example: temporary reductions of Internet speeds, redirection to a landing page until the subscriber contacts the ISP to discuss the matter or reviews and responds to some educational information about copyright, or other measures that the ISP may deem necessary to help resolve the matter”. They mention, “temporary reductions of Internet speeds”, so if this a measure, is it consistent with IETF standards and Network Neutrality obligations? Will services like e-911 calls, video and voice conferencing be affected? (Memorandum of Understanding, 2011)

“redirection to a landing page until the subscriber contacts the ISP to discuss the matter or reviews and responds to some educational information about copyright”, is this an intended interference in the way disrupting functionality of internet browsers?

*The point that needs to be addressed is, Should ISP be authorized to set these technical measures or should IETF be involved with Congress in crafting out standards?*

Packet dropping from the legal side

There is also no legal clarity in § 512 on the aspect of dropping but however RFC 3360 clearly recommends it. So far the protocol agnostic network management is perfectly legal and in accordance with RFC 3360. It should be interesting to explore areas where one could argue, packets as a property right.
Privacy, Wiretapping and similarity with sniffing layers in OSI

With regards to privacy, the ability of a service provider’s network to sniff out information of packets from layers 4 to layers 7 of an OSI is also not addressed. Comcast claims, it does not look at the packet payload, but has the ability to do so. When wiretapping laws exist, they should be a similar parallel or clarity with respect to how many layers of the OSI, does a service provider need to check in sending packets.
Bibliography


Memorandum of Understanding. (2011, July 6). Retrieved August 2, 2011, from Copyright Information:
http://www.copyrightinformation.org/sites/default/files/Momorandum%20of%20Understanding.pdf


