The Future of Video: Challenges in Promoting Competition and Protecting Intellectual Property

Testimony before the Federal Communications Commission
En Banc Hearing on Broadband and the Digital Future
July 21, 2008

Jon M. Peha[1]
Carnegie Mellon University

1 Introduction

Increasing capacity in network infrastructure is poised to fundamentally change the way people watch what we now call "television." Historically, consumers have had to make viewing choices from whatever content is currently being transmitted. Thanks to innovations ranging from Tivo to peer-to-peer networks over the Internet (P2P), it is becoming more common for consumers to collect content locally, and then choose among the content already stored. By the time network infrastructure can support sustained 5 Mb/s downloads to every video screen, each consumer could have the ability to choose from a tremendous range of HDTV-quality videos, at any time, without advance planning. In other words, more "television" content will be pulled by consumers rather than pushed to consumers, and the boundary between television and the Internet could blur.

This shift could potentially bring great advantages for consumers, including greater convenience and diversity of content. The lower cost of content distribution could benefit both consumers and providers of content. There is the potential for greater competition among content providers, and fewer barriers to entry, which would encourage providers to offer innovative and high-quality products at low prices. However, there are also dangers, including the possibility that those who invest funds in the creation of high-quality content will not be able to share sufficiently in the resulting revenues to compensate them for their efforts, and that firms with sufficient market power may become gatekeepers to content in a way that harms consumers. Thus, public policy with respect to intellectual property and network neutrality could have significant impact.

This paper will describe some of the intellectual property issues that will arise as more such content is downloaded over the Internet, probably through some combination of centralized servers, P2P networks, and content distribution networks. Ongoing research at Carnegie Mellon University may provide some useful insights. Some of these issues must ultimately be

[1] Jon M. Peha, Carnegie Mellon University, Professor in the Dept. of Engineering & Public Policy, and the Dept. of Electrical & Computer Engineering, www.ece.cmu.edu/~peha

considered by the Federal Communications Commission in the context of its network neutrality policy. Other issues are left to lawmakers and judges. The primary goal of this paper is to raise questions that must be considered, rather than to answer those questions.

2 Where Intellectual Property Meets Network Neutrality

Intellectual property issues have already entered the network neutrality debate in the context of music. For example, at the most recent FCC En Banc Hearing on "broadband network management practices," one witness [1] described how he benefited from P2P because it is an effective way to legally get hard-to-find music (from barbershop quartets), while another witness [2] described how he might be harmed by P2P because it is an effective way to illegally get copyrighted music without compensating the songwriter. Thus, there is already concern about facilitating the legal flow of music and impeding the illegal flow, a problem that will become more relevant to video content as network capacity increases.

However, there are significant differences between music and video. Many providers of broadband Internet also expect to make significant revenues from today's cable TV service, or variations thereof. These are closed content distribution systems, in which only the service provider is able to decide what content is and is not available. This closed system must compete with the open Internet. If the entity that chooses content in the closed system also plays a role in protecting intellectual property of content on the open system, then intellectual property and competition issues inevitably become intertwined. Indeed, some firms may take actions that are primarily intended to give them a competitive advantage, while justifying those actions to regulators as intellectual property protection. Moreover, even a network service provider[2] that is not offering its own video content could try to extract monopoly rents from other content providers by adding extra charges that are out of proportion with the network resources consumed, and by blocking content when those charges are not paid [3]. (Whether such a strategy would be effective depends in large part on the extent of broadband competition in the future.)

One other difference between music and video is that with video, it is far easier to embed advertising into the content. Thus, the easy dissemination of video content may be more opportunity than threat for video content producers, if the embedded advertisements can somehow be preserved.

3 CMU Findings on Dissemination of Copyrighted Material

Researchers from Carnegie Mellon University have been studying the dissemination of copyrighted material over the Internet, using passive network monitoring [5, 6], surveys and interviews, and other means. This work offers some lessons for policymakers.

[2] A "network service provider" is an entity that operates a communications infrastructure, and offers one or more of communications services, such as broadband Internet, pay-per-view video, broadcast video, and/or telephony.

One portion of this work [5] is an empirical study of actual content transfers at Illinois State University.[3] Using a combination of passive network monitoring tools, including deep packet inspection (DPI) [3], we were able to collect extensive information on students' use of P2P and other applications to legally and illegally transfer content. (To protect privacy, an automated process removes or anonymizes all personally identifiable information from the data before analysis, so no researcher in this study can ever associate any of the data with a specific person, machine, or dorm room.)

We found that many ISU students were involved in the transfer of copyrighted material, from all demographic groups [5]. During the first four-week monitoring period (April 2007), 51% of students who lived on campus were observed using P2P applications, and 42% were seen transferring or attempting to transfer at least one copyrighted music or video title. The mean number of copyrighted titles observed in P2P traffic per student in a typical week was 6, when averaged across all students in the dorms (including non-P2P users). These figures should be seen as lower bounds, because we know our tools missed a substantial fraction of the P2P traffic in that scan. Moreover, not all transfers of copyrighted material involve P2P. (See [5] for full details.) Of course the behavior of college students is not necessarily representative of the behavior of all Internet users, and it is too soon to know whether these students will change their behavior after they graduate and move off campus. Moreover, not all college campuses are the same [6]. Nevertheless, this is an indication that policymakers must take seriously the potential impact of exchanges of copyrighted material.

At the moment, the vast majority of titles that we can identify in the P2P traffic are music. This may partially reflect the nature of our tools. However, it may also be because it takes a very long time to download a video as compared to a song or album. These transfer times will drop dramatically as more of the peers in a peer-to-peer network get high-capacity connections.

We observed more than twice the P2P traffic at ISU in off-peak hours (e.g. 3AM) as compared to peak hours (e.g. 11AM) [5]. It appears that many college students run P2P applications as a passive activity all night, when they might not otherwise use their computers. This is good news for network service providers, as it means P2P consumes fewer resources when those resources are needed most, although it may be bad news for copyright-holders who would prefer that P2P activities stop when human activities stop.

4 What Technology Can Do

While some might like ISPs to wave a wand and block all illegal transfers and no others, technology does not quite allow this. To be effective, policy must be consistent with what

[3] This research was performed in cooperation with the Digital Citizen Project, a broader project undertaken by Illinois State University "to significantly impact illegal piracy of electronically received materials, using a comprehensive approach to confront pervasive attitudes and behaviors in peer-to-peer downloading of movies, music, and media" [4]. ISU's many activities include development of a curriculum to educate students on copyright issues, work with industry leaders to improve educational fair use provisions, new campus policies intended to discourage copyright violations, and this collaboration with Carnegie Mellon researchers involving network monitoring.

technology can actually do. There are at present two basic approaches for detecting transfers of copyrighted material. In the first approach, the network service provider is almost entirely responsible for detecting transfers, using DPI and other technology. Based on our experience [5], this technology may prove quite useful, but its effectiveness is sometimes overstated. Of those users whose P2P traffic is observable by DPI, it was possible to determine which were transferring copyright material by simply monitoring long enough. The technology may be unable to detect copyrighted material after a few hours or a few days. However, after a month of monitoring, most[4] known P2P users were observed transferring at least one copyrighted file. While these numbers refer to P2P traffic, variations of this technique could also be used for other kinds of downloads. Thus, DPI may be a useful tool to measure the extent of file sharing, or to warn users that they might be at risk of lawsuits from copyright-holders.

However, DPI has its limits. Encryption technology can entirely conceal the contents of these transfers, making it impossible to distinguish legal from illegal exchanges. Although many P2P users do not use encryption at present, the option is readily available in the leading P2P applications. Consequently, if DPI were used in conjunction with some sort of punishment for those caught transferring copyrighted material, many users would probably turn encryption on. Thus, neither copyright-holders nor sympathetic policymakers can expect network service providers to fully address the problem of illegal transfers with this type of approach alone.

The second approach to detecting transfers of copyrighted material is to deploy a device that communicates with those who offer or request content, rather than just passively and promiscuously monitoring traffic as it goes by. This is how most enforcement is done today. With this approach, network service providers have no particular advantage. Indeed, it is generally agents of copyright-holders who use this approach to identify the IP addresses of devices that they believe are violating copyright law. The network service providers are involved only to the extent that they later map each IP address to a person.

There are challenges with this approach as well. One is that it is far easier to tell with this approach who is offering copyrighted material to the world than to determine whether someone has actually transferred copyrighted material to or from an unauthorized party. There are ongoing lawsuits over whether the former is sufficient in a court of law [7]. The other problem is that, with existing technology, there is a danger that the wrong person will be identified for a given violation of copyright. For example, it has been shown that it is possible for one user to deliberately make it appear to some (but perhaps not all) of the devices used today for copyright enforcement that another user is involved in illegal transfers [8]. There has also been speculation that in a network where IP addresses change dynamically, it may be possible to identify the IP address of a violator correctly, but to get the timing wrong and then map this IP address to the wrong individual [8]. To the best of my knowledge, this hypothetical problem has not been proven to exist, or disproven. Because the mechanisms used to identify those who infringe copyrights are often proprietary, it is difficult to determine whether this is a serious risk.

We can expect continual improvements in the techniques used to detect illegal transfers of copyrighted material, and in the techniques used to conceal such transfers as well. It is likely that the most effective detection mechanisms will combine elements of both of the approaches

[4] 82.3% in our first scan. See [5] for details.

above. Thus, these hybrid mechanisms would involve both passive monitoring by the network service provider, and active interaction with those who share copyrighted material, probably although not necessarily by some agent of the copyright-holder. Whether such a cooperative arrangement for enforcement is possible, and whether it also brings new and unintended problems, depends on the public policies and business strategies that emerge in the coming years. Some of these issues will be addressed in the next section.

5 Implications for Regulators and Policymakers

The public interest is served by a highly competitive marketplace, where consumers can easily access as well as create and disseminate the content of their choice. The public interest is also served by a system that financially rewards those who create desirable content, so they are motivated to create more. When the communications infrastructure makes the transfer of video content fast and easy, as the transfer of music is today, new challenges will emerge with respect to both of these objectives. As discussed in Section 2, this is particularly difficult because many network service providers will have their own closed system for disseminating video, which gives them a vested interest in limiting the extent to which copyrighted material can flow over the more open portion of the network infrastructure.

Here are some resulting questions that the FCC is likely to face.

Should illegal transfers of legal content be protected under network neutrality principles?

> The FCC has stated that consumers should have access to the legal content of their choice. It is clear that illegal content, e.g. child pornography, is not protected. However, copyright infringement on the Internet typically involves legal content. It is the transfer of this content to unauthorized individuals that is illegal. Would network service providers be prevented from blocking transfers that violate copyright law?

Assuming network service providers can block such transfers, what level of proof must be offered, and to whom should it be offered?

> Users can be erroneously accused of copyright violation, even with an enforcer that is highly motivated to avoid mistakes [8]. The matter is more complicated when the network service provider is also responsible for punishing users by blocking traffic or denying service. First, as described in Section 4, the entity that determines that someone has made copyrighted material available for dissemination may be unaffiliated with the network service provider. To what extent should the network service provider be required to trust this entity? To what extent should it be allowed to trust this entity? Second, the network service provider might benefit when content is blocked that competes with its own offerings. Thus, it may sometimes have incentive to keep the evidentiary bar low. Would doing so ever violate the principle that a consumer can access any legal content she chooses, and if so, under what circumstances?

Assuming network service providers can block such transfers or deny service, must the detection mechanisms be disclosed, at what level of detail, and to whom?

> If too little is known about the detection mechanism, then it may falsely accuse people of copyright violation, and those people may lack information needed to prove their innocence. There is also the danger that these mechanisms will accidentally disrupt other applications, and people operating those applications will lack vital information needed to debug their system.[5] However, if too much is known about the detection mechanism, it may be easier to design systems that illegally transfer information while evading detection.

There are also issues here that involve but probably go beyond the regulator, potentially involving the Courts, Congress, or both.

What constitutes a violation of copyright law on the Internet, and what constitutes sufficient proof of such a violation?

> Perhaps a device merely has to announce that it is willing to share copyrighted material. Perhaps it must share this material with an enforcement device. Perhaps it must share this material with a device other than the enforcement device. Such issues are before the courts now [7], and may eventually fall to Congress. If less evidence is needed to conclude that a violation has occurred, there may be little reason for network service providers to be involved, so attempts to block traffic that have impact on competition in the content markets can be scrutinized more closely. On the other hand, if stronger evidence is needed, this can mean that enforcement depends on the involvement of network service providers.

What are the obligations of an ISP with respect to enforcement of copyright law?

> While the FCC's network neutrality principles may influence what ISPs are allowed to do, intellectual property law will influence what they are required to do. Today, most commercial ISPs cooperate with copyright-holders by linking the IP addresses of alleged offenders to names. In this way, they comply with safe harbor provisions in the Digital Millennium Copyright Act. Some countries are considering mandates for commercial ISPs to play a much greater role than this, while others argue that the level of cooperation seen in the US would violate EU privacy standards [9, 10,11]. Congress is also considering legislation that could force managers of university networks to play a greater role [12, 13, 14]. Obligations on commercial ISPs in the US may change as technology changes, through interpretation of existing law in the

[5] There are complaints that something similar occurred to users of Lotus Notes when Comcast attempted to terminate TCP sessions that carry peer-to-peer traffic.

courts or through new legislation. Such changes could also affect how the FCC defines and applies network neutrality principles.

Under what circumstances are users allowed to transfer copyrighted material under fair use provisions?

At their best, monitoring systems accurately determine when copyrighted materials are transferred, but not whether the specific individuals involved have a right to make this transfer. If some transfers are allowed in the name of fair use, then network providers should not block streams or deny service without somehow checking whether fair use provisions apply. It is presumably not for the FCC to decide policy on fair use, but that policy may also influence FCC decisions regarding when network service providers can block content.

6 References

[1] Robb Topolski, Federal Communications Commission Hearing on Broadband Network Management Practices, Stanford, CA, April 17, 2008.

[2] Rick Carnes, President of Songwriters Guild of America, Federal Communications Commission Hearing on Broadband Network Management Practices, Stanford, CA, April 17, 2008.

[3] J. M. Peha, "The Benefits and Risks of Mandating Network Neutrality, and the Quest for a Balanced Policy," *34th Telecommunications Policy Research Conference*, Sept. 2006. http://www.ece.cmu.edu/~peha/balanced_net_neutrality_policy.pdf

[4] *Digital Citizen Project at Illinois State - Summary of Project*. 2008. www.digitalcitizen.ilstu.edu/summary

[5] A. M. Mateus and J. M. Peha, "Dimensions of P2P and Digital Piracy in a University Campus," *36th Telecommunications Policy Research Conference (TPRC)*, Sept. 2008. www.ece.cmu.edu/~peha/P2P_and_digital_piracy.pdf

[6] Aleecia M. McDonald, Daniel Papasian and J. M. Peha, “Technical and Policy Responses to Spyware,” in preparation.

[7] E. Bangeman, *Judge kills RIAA subpoena: making available not infringement*. Ars Technica, April 3, 2008; http://arstechnica.com/news.ars/post/20080403-judge-kills-riaa-subpoena-making-available-not-infringement.html.

[8] M. Piatek, T. Kohno, A. Krishnamurthy, “Challenges and Directions for Monitoring P2P File Sharing Networks,” University of Washington Technical Report UW-CSE-08-06-01. http://dmca.cs.washington.edu/uwcse_dmca_tr.pdf

[9] N. Anderson, *UK ISPs don't want to play umpire to "three strikes" rule*. Ars Technica, February 15, 2008; http://arstechnica.com/news.ars/post/20080215-uk-isps-dont-want-to-play-umpire-to-three-strikes-rule.html.

[10] E. Bangeman, *France's plan to turn ISPs into copyright cops on track*. Ars Technica, January 28, 2008; http://arstechnica.com/news.ars/post/20080128-frances-plan-to-turn-isps-into-copyright-cops-on-track.html.

[11] P. Meller, *Europe rejects plan to criminalize file-sharing*. InfoWorld, April 10 2008; http://www.infoworld.com/archives/emailPrint.jsp?R=printThis&A=/article/08/04/10/Europe-rejects-plan-to-criminalize-file-sharing_1.html.

[12] *Committee Looks at Technology to Limit Illegal Filesharing*. U.S. House of Representatives, Committee on Science and Technology, Press Release, 2007, June 5. http://science.house.gov/press/PRArticle.aspx?NewsID=1858

[13] *The Internet and the College Campus: How the Entertainment Industry and Higher Education are Working to Combat Illegal Piracy*, 109th Congress House Hearings (SN. 109-58). September, 2006.

[14] *An Update: Piracy on University Networks*, 110th Congress House Hearings (SN. 110-29). March, 2007.