WRITTEN TESTIMONY OF CHRISTOPHER S. YOO

Professor of Law and Communication
Founding Director, Center for Technology, Innovation, and Competition
University of Pennsylvania

Hearing on "Piracy of Live Sports Broadcasting Over the Internet"

Before the Committee on the Judiciary of the United States House of Representatives

December 16, 2009

Mr. Chairman and Members of the Committee, I am grateful for the opportunity to testify on the subject of the piracy of live sports broadcasting. The migration of television broadcasting from analog to digital formats has made it much easier for those interested in pirating content to make nearly perfect copies of video content. To date, most of the attention has been focused on prerecorded television programming, such as movies and most television shows. Today's hearing focuses welcome attention on the unique problems and challenges posed by the piracy live television.

I will begin my remarks by briefly describing how unauthorized copies of video content are made and distributed. I will then outline the various technical and legal measures available to curb the unauthorized dissemination of live television content.

Copying Live Television Content

A wide range of companies offer devices that that can hook up to cable and satellite television set-top boxes and copy high definition television programming directly to any personal computer. For example, Hauppauge offers an HD PVR for $249. These devices typically function by connecting to the component video ports on the set-top box. Component video is an analog format. Although these analog signals cannot take advantage of digital compression

techniques, the signals can be recompressed with only a relatively small loss of fidelity. Copy protection systems exist for analog formats. They are generally relatively easy to evade and designed to prevent copying of DVDs and other forms of prerecorded content.

Devices sold today also typically have HDMI and DVI ports that employ exclusively digital formats. Because they employ digital formats, they can incorporate more sophisticated copy protection known as High-bandwidth Digital Content Protection (HDCP), which requires certain technology to be built into the television sets themselves. Although HDMI capture cards and other devices exist that are capable of evading HDCP and can copy protected programming from HDMI ports, they remain relatively rare.

Distributing Live Television Content

Once television programming has been captured and stored on a computer, the person wishing to share the unauthorized copy must find a way to distribute it. The traditional means for doing so is streaming video, in which the copier establishes an Internet connection with interested viewers and delivers the programming through a continuous flow of data.

Those making unauthorized copies of television programming have increasingly used peer-to-peer systems to distribute them. In a peer-to-peer system, the content is saved in a file that is stored by multiple end users throughout the network. Because peer-to-peer systems require that programs be recorded, then stored, and then accessed, they have generally functioned better for distributing prerecorded content, such as movies, than for programming being broadcast in real time. More recently, peer-to-peer systems have begun saving live programming in short segments of approximately ten seconds. This has enabled those making unauthorized copies to distribute the content without having to wait until the end of the program and has enabled viewers to view these programs on an almost-live time frame simply by accessing a

series of small files rather than one large one. Websites exist that allow end users to view a wide range of live sports programming, much of which is being offered on a pay-per-view basis. (For one example, see www.atdhe.net.) Observers report that peer-to-peer distribution of live television has become a particularly serious problem in China.

Possible Technical Measures to Curb Piracy of Live Television

A number of technical measures exist for curbing the piracy of television programming. For example, it is possible to use the characteristics of particular video content to generate a "fingerprint" of the content. Video fingerprints remain effective even if the content has been abridged or has undergone significant editing. Network providers can use deep packet inspection to examine traffic and see if it carries the fingerprint to identify content that is likely to be pirated. Content providers can also embed a "watermark" within the content that can identify the particular source of any particular copy. A number of firms exist that scour the Internet and inform content owners whenever they locate unauthorized copies

Unfortunately, all of these solutions are less effective for live television than for prerecorded television. For example, any Internet service provider (ISP) using video fingerprints to filter traffic passing through its network must receive a constant stream of updates of the fingerprints. The problem is that fingerprints are based on the characteristics of the actual program. As a result, they cannot be determined until the program has actually been produced. When a program has been prerecorded, it is a simple matter to disseminate the fingerprint to the relevant databases prior to the public release of the content. For live programming, however, this is impossible. Currently, the services that host video fingerprints typically update their databases only once a day or perhaps once an hour. Even if a service wished to send more frequent updates, propagating information about the fingerprints takes time and would almost certainly

not be disseminated until after the live television program has already been made available to the public and thus available for unauthorized copying.

Although watermarks can be determined in advance, watermarking is also harder to verify in real time. As a result, it is relatively ineffective as tool for identifying piracy of live television programming. Instead, watermarking is best used as an after-the-fact, forensic tool to determine which actor was responsible for allowing the unauthorized copy to be made. Although useful for curbing unauthorized copying and distribution of prerecorded content, watermarking is less helpful in curbing piracy of live television programming, where most of the value lies in being able to view the event as it occurs.

Perhaps most importantly, those seeking to distribute unauthorized copying can defeat both fingerprinting and watermarking by encrypting their data streams. Networks have responded by interjecting themselves as a "man in the middle" in order to receive the encryption keys as the session is being established. Peer-to-peer systems are also trying to employ "darknets," in which people must be invited by someone else willing to vouch that the person being added to the network is not going to sue them for copyright infringement before they are allowed to participate in the network. Content owners in turn attempt to infiltrate these darknets by posing as someone the others sharing illegally pirated content through peer-to-peer networks can trust. The result is an endless cat-and-mouse game in which both sides spend significant resources in a series of moves and countermoves in an attempt to stay one jump ahead of the other side.

Possible Legal Measures to Curb Piracy of Live Television

These technical measures can be complemented and reinforced through a series of legal measures to curb piracy of live television content. The distributed nature of the Internet makes it

difficult, if not impossible, to target the private individuals who are actually making the copies. Consequently, legal responses generally focus on commercial actors that facilitate illegal piracy, such as those firms that manufacture the devices that make the actual copies and the websites that inform viewers where they can find the copies.

For example, manufacturers of HDMI capture cards equipped to evade the copy protection provided by HDCP may be subject to liability under the Digital Millennium Copyright Act (DMCA).[1] In addition, firms such as Grokster and Pirate Bay that serve as focal points for information about where unauthorized copies are available for download have been increasingly subject to vicarious liability for their role in facilitating piracy. The fact that viewers of unauthorized copies of live television programs similarly depend on websites and other key intermediaries to identify and provide access to these video streams suggests the possibility of pursuing similar strategies to curb piracy in this context as well.

Finally, there is the extent to which network providers should bear legal responsibility for curbing unauthorized copies. Under the DMCA, network providers are largely immune from liability for copyright infringement so long as they maintain policies to terminate repeat infringers and accommodate standard technical measures that protect against copyright infringement.[2] In order to receive DMCA immunity, the network provider must also expeditiously remove material claimed to be infringing.[3] To date, the law has been reluctant to impose substantial liability on network providers or to require them to filter for content that infringes copyright, largely out of concern that the cost of doing so would deter the deployment of network services. There are some indications, however, of a change in heart. For example, in

---

1 17 U.S.C. § 1201.
2 17 U.S.C. § 512(i)(1).
3 17 U.S.C. § 512(c)(1)(C).

the *Grokster* case, the Supreme Court pointed to the fact that neither Grokster nor Streamcast "attempted to develop filtering tools or other mechanisms to diminish the infringing activity using their software" as evidence that they were inducing their customers to use their technology to violate the copyright laws.[4] As the cost of video fingerprinting has fallen, some courts have begun to explore the possibility of requiring ISPs to filter for piracy. For example, one Belgian court concluded that the cost of filtering had dropped to the point where it was appropriate to issue an injunction ordering an ISP to deploy software to filter for copyright infringing content.[5] The court later lifted the injunction on October 24, 2008, on the grounds that the filtering software was not yet ready to perform these functions.[6] The possibility remains that courts may begin to mandate filtering for piracy once such software is ready for deployment.

Finally, the European Parliament has authorized EU member states to enact laws disconnecting individuals from the Internet. In response, the French National Assembly has enacted a "three strikes" law requiring ISPs to give two warnings and then cutoff subscribers who repeatedly violate the copyright laws. The UK is reportedly testing a similar program that will be fully deployed in 2011.

The Future

Speculating about the future is particularly difficult in an industry as technologically dynamic and diverse as the Internet. The evidence suggests that the solutions to the problems of piracy of live sports programming are likely to be complex and likely to involve a wide variety of stakeholders, including content owners, device manufacturers, network providers, websites,

---

4 *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 939 (2005).

5 *SABAM v. S.A. Tiscali (Scarlet)*, No. 04/8975/A (Dist. Ct. Brussels June 29, 2007), *reprinted in* 25 CARDOZO ARTS & ENT. L.J. 1279 (Fran Mady et al. trans., 2008).

6 T.J. McIntyre, *SABAM v. Scarlet: Belgian ISP Released from Obligation to Filter Network for Illegal Downloads*, *at* http://www.tjmcintyre.com/2008/10/sabam-v-scarlet-belgian-isp-released.html (Oct. 26, 2008).

and software firms. The problem is that those who will benefit from implementing solutions to the piracy of live television are often different from those who will bear the costs. It is thus quite possible that Congress may need to step in to create a solution to a complicated and multifaceted policy problem.