THE ENTERTAINMENT INDUSTRY: What Keeps In House Counsel Up at Night?

Panelists: John McCoy, Chief Compliance Officer, Fox Filmed Entertainment
Marlo Carruth, Assistant Chief Counsel, Studio Legal Distribution

Moderator: Sandra J. Wunderlich, Tucker Ellis LLP, St. Louis, MO

The widespread use of digital technology in the entertainment industry has had a significant impact on how movies and television programs are distributed and consumed by the public. Technology is rapidly changing the access points for consumers, and the law's best efforts to protect the intellectual property involved cannot keep pace with the technological advances. Rather than transferring a physical product, the consumer now can obtain access to films and programs through video streaming or downloading electronic files, which allows for global distribution at the touch of a button. While the ease of product delivery is convenient for the seller and the consumer, these methods of distribution create challenges for the entertainment industry, including the constant efforts to prevent online piracy of these digital files, and to prevent cyberattacks that aim to steal incredibly valuable intellectual property.

The Cost of Online Piracy:

The Motion Picture Association of America (MPAA) reports that its members lose billions of dollars every year due to online piracy. This figure has been estimated to be as high as $20 billion for the entire movie industry. The best estimates for last year indicate that there were 450 million downloads of pirated films, television and video shows in the U.S., and 4.5 billion worldwide. And, Google reports having processed over 78 million piracy removal requests in just one month. Clearly, this is a widespread problem.

Although most countries have anti-piracy laws, enforcement is the challenge. Locating the actual infringers can be very difficult, and once the movie or television program is posted online, the damage cannot be undone. Copyright holders prosecute the infringers when they are found, but they also direct their efforts to holding the Internet Service Providers (ISPs) accountable if they support the unauthorized copying or transfer of files. The Supreme Court has held that file-sharing services that contribute to the infringement can be held liable. *See Metro-Goldwyn-Mayer Studios, Inc., et al., v. Grokster, Ltd., et al.,* 544 U.S. 903 (2005).

Anti-Piracy Laws:

In 1998, the United States enacted the Digital Millennium Copyright Act (DMCA), which adopted two major international treaties of the World Intellectual Property Organization (WIPO). The law included a multitude of policy changes, but a small number of major changes particularly impacted the availability of online content. The law strengthened penalties for violating copyright law, made it illegal to circumvent anti-piracy controls (even if the copyright is not violated after this circumvention), and added liability against those who assist in the distribution of copyrighted materials. Perhaps its largest impact was the creation of a system of notices that require removal of the infringing material, and subsequent lawsuits against those hosting copyrighted material, which is still in place today.

Due to the difficulty in locating the actual infringers, the copyright owners have strengthened their efforts to impose liability upon online intermediaries that facilitate the infringement. Both the DMCA and the European E-Commerce Directive (2000) provide immunity for copyright infringement for online intermediaries if (a) they do not know about the infringement, and (b) if they take action after they are notified of the infringing content, which is often referred to as the "safe harbor" provision. Many believe the "safe harbor" provision is too lenient, and the DMCA does not go far enough to protect the owners of the copyrights.

Several organizations representing artists and entertainment companies have pushed for changes to the DMCA safe harbor provision to further combat online piracy. Critics note that the law was passed twenty years ago and technology has advanced significantly since that time. With the advancements in technology comes an increase in piracy. Organizations that represent the copyright holders advocate a stricter procedure whereby the copyright holder gives the ISP notice of the infringement, and the ISP is required to take it down, and keep it down. Right now, the ISPs are required to take down the infringing material upon receipt of the notice, but as soon as one link is taken down, there is another link on another site. It is a constant battle that requires constant vigilance. Proponents believe the key is the "stay down" portion of this equation, particularly as it relates to content that has not been released to the public by the copyright holder. They believe ISPs should be required to locate all links, remove them, and continually search for any additional links that are added.

Effective in 1995, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) is an international agreement between all of the members of the World Trade Organization (WTO). It establishes minimum standards that each member nation must impose for the protection of intellectual property among its member nations. For example, TRIPS requires its member nations to pass laws to establish protection of copyrights, trademarks, trade dress, patents, and confidential information that include enforcement rights and procedures.

With respect to copyright infringement, Article 50 of TRIPs requires that member nations allow their courts to issue injunctions and to order the destruction of infringing products, and to award damages. Article 61 of TRIPs requires the establishment of criminal procedures and penalties in cases of "willful trademark counterfeiting or copyright piracy on a commercial scale." The U.S. allows for criminal charges where the infringer acted "for the purpose of commercial advantage or private financial gain." 17 U.S.C. § 506. It must be "willful infringement" for criminal liability to attach. Punishment may include jail time or fines, with a maximum penalty of $150,000 per instance of infringement.

In 2011, Australia, Canada, Japan, Morocco, New Zealand, Singapore, South Korea, and the United States signed the Anti-Counterfeiting Trade Agreement (ACTA) to establish international standards for the enforcement of intellectual property rights. The goal of ACTA is to target counterfeit goods and copyright infringement through the Internet. This includes sale of counterfeit goods, but also illegal downloads and streaming. In 2012, Mexico and the European Union signed ACTA. ACTA requires that signatory countries add criminal penalties for copyright infringement.

Legislatures proposed the Stop Online Piracy Act (SOPA) in an effort to expand the definition of "willful" infringement, and add felony charges for infringement and sale of counterfeit goods through the Internet, but this bill was controversial given the ability to shut down a website accused of piracy. The U.S. recognizes the need to stop online piracy, recognizing the problem will only grow larger, but must balance the interests of legitimate smaller businesses that may be negatively impacted if too much power to control the Internet is invested in the hands are larger players on the Internet.

International Trade Commission

In a closely watched case, the Federal Circuit determined that the International Trade Commission (ITC) does not have the authority to prevent digital importation of infringing files via the Internet. The ITC has been a powerful resource for patent owners to prevent the importation of infringing goods into the U.S. The Federal Circuit Court of Appeals was presented with the issue of whether the ITC could and should prevent the importation of infringing articles, including digital files, in *ClearCorrect Operating, LLC v. ITC and Align Technology, Inc.*, 810 F.3d 1283 (Fed. Cir. 2015). In that decision, the Federal Circuit reversed the ITC's holding that its power extends to "articles that infringe," including digitally transmitted data. The case involved three dimensional printers being used to form aligners to straighten teeth for orthodontia treatment. The dentist and the alleged infringer were exchanging digital files that could be used to create braces by using a three dimensional printer. Align Technology alleged that this practice violated several different patents it owned. But, the only "importation" into the U.S. were the digital files used to create the braces using the three dimensional printer.

The Federal Circuit relied upon Section 337 of the U.S. Tariff Act to hold that the ITC's jurisdiction is limited to "material things." Opponents argued that the U.S. Tariff Act does not differentiate between infringing goods that are imported electronically versus physically, and that the law must be read to keep up with the changes in technology where things that were previously in "material" form are now digitally files. In spite of this, the Federal Circuit ruled that Congress would need to amend the authority of the ITC if it wanted to extend its authority to police infringing digital files brought into the U.S. Thus, it held that ITC did not have jurisdiction over digital files and that the United States District Courts were the only option to address infringement of digital files. The ITC filed a request for rehearing en banc, but that was denied. The parties initially sought an extension of time to file a Petition for Writ of Certiorari for review by the Supreme Court, but ultimately did not do so. The entertainment and software industries had hoped the ITC might serve as another resource to combat online piracy, but for now, the ITC is not tasked with that authority.

This year, a large group of entertainment companies have joined forces to combat the growing problem of piracy by creating the Alliance for Creativity and Entertainment. Even though they are generally competitors, this group of companies supports initiatives to combat piracy on all levels including education, and lobbying for stricter laws. The group plans to work closely with law enforcement to pursue and prosecute infringers to the fullest extent allowed by law, but also to obtain voluntary compliance among responsible ISPs, and platforms to assist in the prevention of infringement. This may be the only way that entertainment companies can gain ground in the war against online piracy.

Panelists will discuss their efforts in combatting the acts of online piracy, but also managing the impact this crime has on their revenue stream and the profitability of their products.

Cyberattacks impacting the Entertainment Industry:

Cyberattacks or data breaches by hackers have impacted many industries. It seems like there is an announcement of a significant data breach for large companies every day. And, the entertainment industry is no different.

Earlier this year, Disney reported that criminals claimed to have hacked into its database, and demanded ransom to be paid in bitcoin or it would release one of the studio's forthcoming movies online. Disney made it clear that it refused to pay the ransom, and immediately enlisted the assistance of law enforcement. Even after Disney refused to pay the ransom, the new movie that allegedly had been compromised was not released. It is widely believed that the demand for ransom from Disney was a hoax. But, the month before, there was a different result. Hackers stole the fifth season of Orange is the New Black and demanded ransom from Netflix to prevent its release. When Netflix refused to pay, the hackers uploaded the program online just as they had threatened. Although law enforcement is involved, no arrests have been made.

HBO was also the victim of a deliberate and widespread cyberattack, which stole thousands of its copyrighted materials. After threatening to leak new programs if a ransom was not paid, the hackers leaked upcoming episodes of HBO programs as well as a script for a "Game of Thrones" episode, among other things. HBO worked closely with law enforcement and just last month, the U.S. Attorney's office in New York announced charges against an Iranian national for the hacking of HBO's servers. He is charged with computer fraud, as well as wire fraud, interstate transmission of an extortionate communication, and aggravated identity theft. Although the Iranian national cannot be extradited to the United States for prosecution, the indictment may prevent that individual from freely moving around the world.

In 1986, the U.S. adopted the Computer Fraud and Abuse Act (CFAA), which amended existing computer fraud laws within the Comprehensive Crime Control Act of 1984. Put simply, the law prohibits unauthorized access to computer files. CFAA not only criminalizes certain behavior, but it allows for a private right of action for violation of the law. CFAA included provisions that make it a crime to distribute malicious code (viruses), or sell passwords to allow criminals unauthorized access to computers. Congress has amended the CFAA multiple times, and most recently in 2008 with the Identity Theft Enforcement and Restitution Act.

Panelists will discuss efforts to prevent cyberattacks and strategies for dealing with them when they occur.