
The Stop Online Piracy Act and the High Seas of the Internet Age

A few weeks ago, Congress quickly shelved the Stop Online Piracy Act (SOPA) and the Protect IP Act (PIPA) after incurring vocal public outrage.

Hayes Hunt and Brian Kint

2012-02-15 12:00:00 AM

A few weeks ago, Congress quickly shelved the Stop Online Piracy Act (SOPA) and the Protect IP Act (PIPA) after incurring vocal public outrage led by Web giants such as Google and Wikipedia. SOPA and PIPA both sought to require the blacklisting of websites that facilitate online piracy. For example, search engines would have to exclude offending sites from search results and third-party payment processing companies like PayPal could not do business with them.

As originally drafted, the laws would have required Internet service providers to block offending websites — an Internet "death sentence." The controversy over SOPA and PIPA puts into focus the tension between intellectual property rights and First Amendment free speech realities that many general counsel should bear in mind as their companies navigate the high seas of the Internet Age.

Although the tension between intellectual property rights and free speech has always been present, in the past it largely was reconciled through limited enforcement. In the late 18th century, only the most dedicated infringers would have taken the time to undertake the arduous process of reproducing another's work. For example, early printing presses could reproduce a few hundred pages an hour, at best, and the operator had to set the type by hand for each page.

Throughout the years, however, technological advances made the reproduction process quicker and easier. By the end of the 20th century, technologies such as the photocopier, the cassette recorder and the VCR gave people the ability to reproduce entire works with the push of a button. Still, these reproductions were of inferior quality. Think about a bootleg copy of Bruce Springsteen's "Born in the U.S.A." or the ubiquitous "mix tape" of the 1980s. Enforcement remained lax and focused on large-scale commercial infringers, not on individual consumers.

Digital technology and the advent of the Internet changed everything. Digital technologies such as CDs, MP3s and MPEGs allowed users to copy a work an infinite number of times with no reduction in quality. They could make numerous copies with a few clicks of a mouse. Then, the Internet gave them the ability to distribute these copies to a worldwide audience. No longer were individual infringers a few isolated households with the money to purchase two VCRs and make a copy of their three-day rental of "Raiders of the Lost Ark." Instead, a single person could distribute a high-quality reproduction of a song, movie, book or picture to people across the globe, instantly and at little cost.

This new reality led to a change in civil enforcement strategy for many companies. Instead of focusing on large-scale commercial infringement, many industries began to target consumers of pirated material. Their litigation strategy was intended to deter individuals from sharing files across the Internet. The prototypical example of this strategy is *Sony BMG Music Entertainment v. Tenenbaum* , in which a number of recording companies obtained a $675,000 judgment against a college student who illegally downloaded 30 songs. Joel Tenenbaum had downloaded the songs for his personal use through the peer-to-peer file sharing application Kazaa. He was found liable despite his argument that private, noncommercial copying constitutes permitted "fair use" under federal copyright laws. The case is currently in front of the U.S. District Court for the District of Massachusetts to determine if the damages awarded should be reduced.

Technological changes created new challenges in criminal enforcement as well, as illustrated by a recent case. On Jan. 19, federal prosecutors seized and shut down the website Megaupload.com and charged seven of its executives with Internet piracy. Megaupload is a website that allows users to upload and transfer large files, often music or movies. The website is based out of Hong Kong, but some of the allegedly pirated content was hosted in Virginia. None of the seven executives charged is a U.S. citizen or resident. If convicted, they face up to 20 years in prison. The case raises three of the most pertinent issues of contemporary anti-piracy law.

First, it raises questions of legitimate use. Usually, technologies that "facilitate" piracy have legitimate, noninfringing uses as well. For example, file-hosting services — such as Megaupload — allow users to store large files in a "Web locker" so that anyone, anywhere, can access them, as long as they have a computer with an Internet connection. This technology is important to businesses in a global economy and it will become even more important as data moves off of individual computers and into the aptly named "cloud." Nevertheless, skeptics argue that professed legitimate uses are simply a front to disguise the true intent of facilitating or encouraging piracy.

This dilemma is not new. Since the 1984 U.S. Supreme Court case *Sony Corp. of America v. Universal City Studios Inc.* ,courts have struggled to formulate and apply a standard of liability for manufacturers of products or technologies asserted to be aiding copyright infringement. There, the film industry attempted to hold VCR manufacturers liable for "contributory infringement" for providing a technology that consumers could use to record and copy movies. The court ruled that the manufacturers were not liable because the device had significant noninfringing uses. Yet, the case is not so clear when considering Internet technology providers that — unlike VCR manufacturers — often route activity through centralized servers, allowing them to control consumer activity in a way that was impossible in the past.

That leads to the second issue raised by the Megaupload case: the responsibility of a website provider for the content of the site. The Internet is inherently open and collaborative. Many websites simply provide a forum and users provide the content. For example, YouTube's content is primarily user-uploaded video clips. And even where the website provider delivers the majority of the content, users are often invited to post comments and discuss the content. User message boards and user-generated content are commonplace on news sites, blogs and social networking sites. This environment begs the question of what responsibility a website provider has to monitor the site and remove offending content. Courts and the law are struggling to draw this line in a way that effectively balances intellectual property rights with the openness of the Internet.

Finally, the case raises issues of jurisdiction in the Internet Age. For the most part, intellectual property laws are limited geographically. What is legal in one country may be forbidden in another. Nevertheless, the Internet allows businesses to reach across jurisdictional lines while maintaining a physical presence in a

single country. While it seems odd to believe that a company can subject itself to every jurisdiction in the world simply by posting something to the Internet, it seems equally odd to believe that a company can shield itself from all liability simply by running its operations from a country with weak intellectual property laws. Consequently, Internet anti-piracy cases raise questions of exactly where a violation occurred, what country's intellectual property law applies and whether a country can enforce its laws against a particular entity or person. These issues have blurred traditional jurisdictional lines and concepts of due process.

Many of these issues are not unique to intellectual property law. Yet, the digital age and the Internet revolution undoubtedly have made the world of intellectual property and anti-piracy more complex than ever. Company decision-makers need to completely understand the law, the company's Internet presence and the ways consumers use the websites and online services the company provides. Executives and corporate counsel must manage the business of the Internet. This task requires them to recognize and negotiate many pitfalls, obstacles and booby traps — much like Indiana Jones as he searched for the Ark of the Covenant.

Hayes Hunt *is a member of **Cozen O'Connor** in the firm's commercial litigation and criminal defense and government investigations practice groups. He is the creator of "From the Sidebar," a blog dedicated to trial, litigation and the practice of law. He has tried numerous cases to verdict in both criminal and civil matters and is an adjunct professor of law at Temple University. He can be reached at hhunt@cozen.com.*

Brian Kint *is an associate attorney in the litigation group at the firm. A graduate of Harvard Law School, he has represented clients in numerous areas, including criminal defense and government investigations. He can be reached at bkint@cozen.com*