DOI:10.1145/2063176.2063190

Randal C. Picker

Law and Technology
The Yin and Yang of Copyright and Technology

Examining the recurring conflicts between copyright and technology from piano rolls to domain-name filtering.

The emergence of the Internet has put enormous pressure on the rights model of U.S. copyright law. That model is premised on the notion that copyright holders are entitled to control the making of copies of their works, but technology has made that control somewhere between fragile and nonexistent. Content creators have struggled to restore the control assumed by copyright law. Two recent developments, one pending federal legislation and the second an industry-wide agreement between Internet service providers and content distributors, provide new looks at this ongoing issue.

Technology and copyright have a complex relationship. New waves of technology have created novel expressive opportunities and dramatic improvements in the ability to distribute copyrighted works. But new technology rarely asks permission, and with each technical advance, we have seen new opportunities and new clashes. Perforated rolls for player pianos in the early 1900s came from sheet music and roll producers were not eager to write checks to copyright holders. Radio saw recorded music as a way to fill the airways even though disks came with a legend stating that the music was not licensed for radio broadcast. And the VCR introduced a new vocabulary—time shifting—and the chance to watch TV on your schedule, not broadcasters' schedules. It did so without offering any compensation to broadcasters or show producers and even created the risk that the financing model for free broadcast TV would be put at risk by viewers with nimble fingers who fast-forwarded through commercials.

The rights model of the law has not changed—authors are entitled to control copying—but the practical ability to enforce that right has shrunk.

Since at least the advent of Napster, the music industry has struggled to find a strategy to control illegal downloads of music. Technology made it very easy to rip CDs and share the results with the world. The music industry responded with lawsuits, first against Napster, Aimster, and Grokster, and then against individual consumers, leading to prominent examples such as the ongoing saga of Jammie Thomas-Rasset. The suits have been on the whole quite successful, at least as measured by the standards that lawyers use. Grokster lost 9-0 on the question of whether it might be liable for inducing copyright infringement (there was much more division on the question of how the U.S. Supreme Court's prior *Sony* case should apply to this situation). Thomas-Rasset has faced juries multiple times and each time jurors have come back with damage awards—the first time $1.92 million and second time $1.5 million—that judges found too high.

Notwithstanding all of that, the

music industry sees these as paper victories, as file sharing has continued largely unabated. In some basic sense, law has failed the music industry. Technology has changed the integrity associated with distributing copies of copyrighted works by making copying easy and worldwide distribution instantaneous. To distribute a copy of the work is to put the means of production into the hands of consumers.

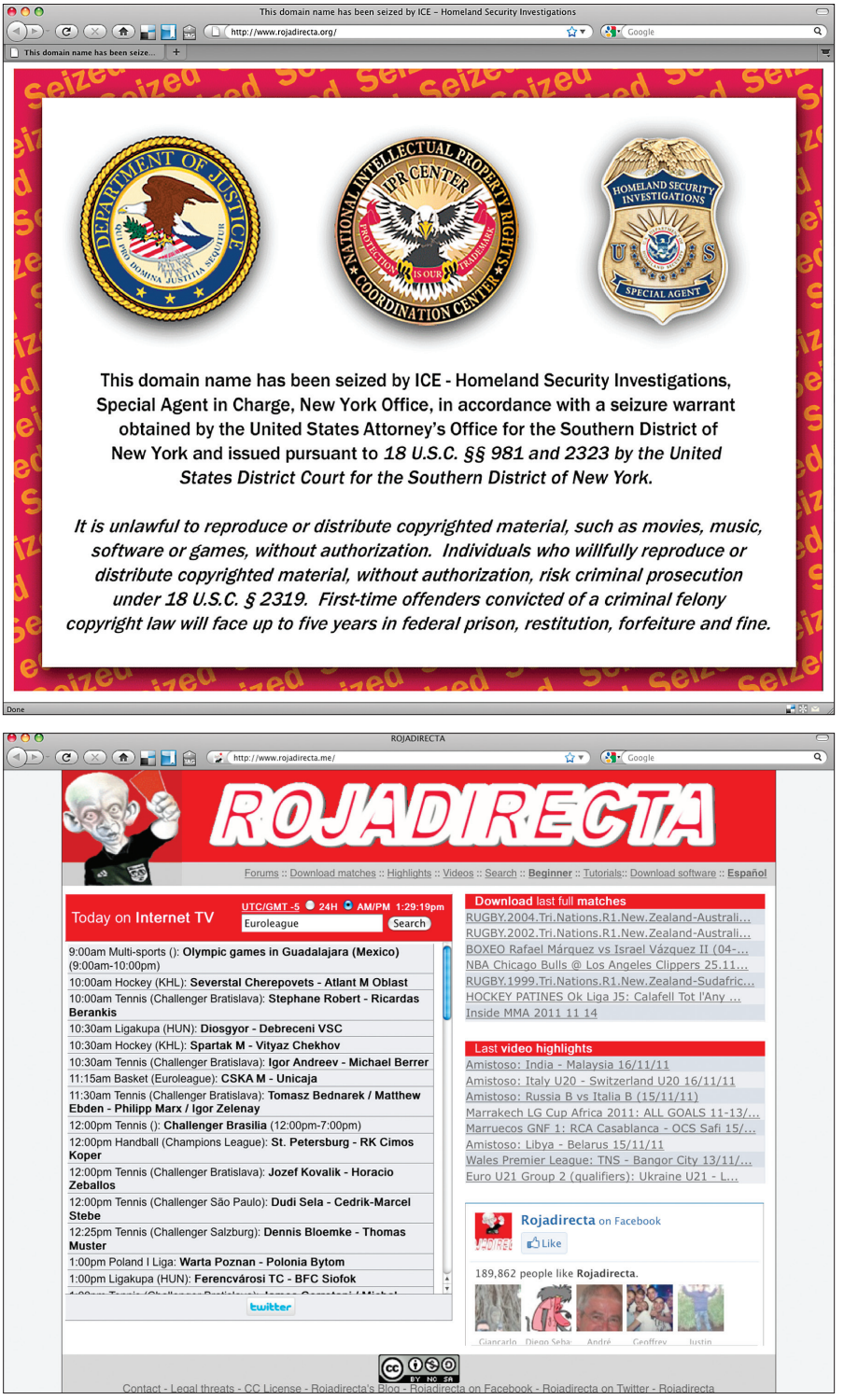
The rights model of the law has not changed—authors are entitled to control copying—but the practical ability to enforce that right has shrunk. The music industry started by chasing firms that were facilitating peer-to-peer file swapping. But this was like chasing quicksilver: even if you got your hands on one version, another would quickly reappear and the hive-mind of the P2P networks would reorganize around the new version.

The litigation clock is wildly out of sync with the speed of P2P organization. Ordinary law enforcement scales poorly and it is easy to see why the content industry would like a scalable way to enforce the key right to control whether copies are made of copyrighted works.

The Rojadirecta Case

In late 2008, Congress passed the Prioritizing Resources and Organization for Intellectual Property Act of 2008. The sole virtue of such a clumsy name is that it shortens to the PRO IP Act. The new act made it possible for the federal government to seize domain names associated with Web sites where allegedly infringing behavior was taking place or being facilitated. And seize it has. On June 30, 2010, the U.S. Immigration and Customs Enforcement bureau launched Operation in Our Sites and seized nine domain names and physical assets connected to commercial movie and television piracy Web sites. The program has expanded with additional domain name seizures for 77 sites in November, 2010 and with three additional sets of seizures of domain names through mid-2011.

Take a closer look at one of these cases. On February 1, 2011, the U.S. government seized the rojadirecta.com and rojadirecta.org domain names. Before the seizures, rojadirecta.com and rojadirecta.org offered up a guide to Internet TV focusing on sports (a lot of what the U.S. calls soccer but the rest of the world calls football). Like the early Napster, Rojadirecta offers links, not direct hosting, to facilitate what it calls P2P TV.



Home pages for rojadirecta.com (top) and rojadirecta.me (below).

But if you go to those domain names today, when you type the .com or .org sites into a browser after the seizure, you are not offered links to the beautiful game. The URL bar for your browser will indicate you have indeed reached your intended destination, but when you look at your screen you see three U.S. governmental enforcement seals. The rest of the page briefly sets out the basis for the seizure—a search warrant under two federal statutes—and states that copyright infringement can be a federal crime.

Search rojadirecta.org on the whois database. The current registrant for the domain name is the U.S. Department of Homeland Security with corresponding physical addresses, email addresses, and phone numbers. This is what a domain name seizure looks like. Prior to the seizure, the registrar Go Daddy dealt with Rojadirecta as its customer, but now the federal government has been substituted as its customer and the feds exercise control over the domain name.

But there is more to the story, of course. You do not have to type in a domain name to reach a Web site. That is just a convenience for us humans. You can type in an IP address directly and the seizure of rojadirecta.org means nothing for direct connection to the Rojadirecta Web site through the IP address. And, if that is too clumsy, Rojadirecta solved that problem by setting up new domain names offshore, including relocating to Spain at rojadirecta.es. Rojadirecta immediately announced its new domain names through its accounts on Facebook and Twitter and was back up and running. That is not to say that Rojadirecta does not want its original domain names back—it does and is in litigation over that—but the move to offshore domain names makes clear why the Pro IP Act is not the be-all and end-all for protecting copyrights.

The litigation over the Rojadirecta domain names is at a very early stage. In August, 2011, a federal court rejected Rojadirecta's preliminary efforts to get back its domain names. Part of this analysis turned on the injury that Rojadirecta was suffering from not having access to the old domain names and the court found that that injury was minimal. Why? Because Rojadirecta had been able to set up new domain names outside of the reach of U.S. officials and Rojadirecta could easily inform its users about its new locations. So, to be a tad cynical, the complete ineffectiveness of the seizure meant it did not matter in the short run that Rojadirecta could not use its original domain names. Rojadirecta sought to press a First Amendment claim, but the court left that for subsequent litigation, again on the view that the speech was not blocked but was instead just displaced to a new location.

The Rojadirecta saga should make clear why the content industry is looking for new enforcement tools.

New Enforcement Tools

The Rojadirecta saga should make clear why the content industry is looking for new enforcement tools. New legislation passed in 2008 in the form of the Pro IP Act, domain names seized and yet the activity continues elsewhere outside of the country. What might a solution look like? A technological approach by companies with the market position and financial stakes to make something work, companies with something to lose if they fail to comply with their obligations. Digital rights management was a technical response, but one that embedded the technical protection in the digital object itself, and not in the Internet's infrastructure. Something based in the U.S., so the firms can't just exit overseas. The natural target might be big firms with bottlenecks. This sounds like Internet service providers, search engines, and the like. It sounds like, in fact, S.968, the draft act on Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011—the Protect IP Act for those of you quick with abbreviations—and the industry-wide memorandum of understanding implemented in July, 2011. (And the House of Representatives has put its own dog in the fight with H.R. 3261, the Stop Online Piracy Act.)

Start with the latter and call it the ISP Memorandum. This is an agreement between key players in the content industry—the Recording Industry Association of America, the Motion Picture Association of America, and a number of the corporate members of the RIAA and the MPPA—and the leading Internet service providers, including corporate entities for Verizon, Comcast, and Time Warner Cable (but without consumers at the bargaining table). The core of the agreement is a graduated six-step protocol for Internet service providers to respond to customers thought to be engaging in IP infringement. The protocol calls for education of offending consumers through steps such as temporary landing pages before consumers are able to access the Internet generally. Education is backed by a variety of mitigation measures directed at degrading the quality of the service delivered by the Internet service provider such as reduction in download and upload speeds.

The Protect IP Act would impose obligations on intermediaries and infrastructure providers to make it more difficult to find and get to sites that are, in the language of the bill, "dedicated to infringing activities." The idea behind this is simple: if technology has created the problem of easy file sharing, technology also should provide the solution. This would include, after action by the federal government in court, blocking domain names from resolving to the matching IP address—DNS filtering—and not serving up links to infringing Web sites. And there is no shortage of criticism of these provisions: many law professors are up in arms about the First Amendment, while a white paper by leading technologists suggests the act would accomplish little while interfering with efforts to roll out the new DNS Security Extensions.

Conclusion

The ISP Memorandum and the draft acts represent the current bleeding edge in the ongoing struggle between copyright and technology. We have moved from piano rolls to DNSSEC, but the conflicts recur. The legal regime gives copyright holders the right to control the making of copies, but no one told that to technology. Technological engineering is frequently easier to do than institutional engineering and yet these systems need to coevolve and to do that we need to talk across the disciplines in a coherent way. If we fail to do that, we will produce a sloppy result that will not accomplish anything for law or for technology. C

Randal C. Picker (r-picker@uchicago.edu) is Paul and Theo Leffmann Professor of Commercial Law at The University of Chicago Law School and Senior Fellow at The Computation Institute of the University of Chicago and Argonne National Laboratory.