Protecting the Past by Constricting the Future: The Proposed Anti-Counterfeiting Trade Agreement's Effect on Innovation

Stephen Goldmeier, May 2010

I. Introduction

The Internet's life has been a messy one, without clear beginnings and chapters. But one of the themes of that story has been the freedom to innovate. The open TCP/IP protocols that made easy connection to the vast network encouraged innovators to plug in their new Internet technologies and immediately try radically new things. And the accessible, inexpensive transfer of large amounts of data has led to such innovative ranging from online encyclopedias (Wikipedia)[1] to voice and video chat (Skype)[2] to a device for transmitting virtual hugs to partners across the planet[3].

It is this attitude of openness that has made the Internet the powerful tool it is today.[4] But that openness has come at a price: illegal, copyright infringing activities are easier than ever using Internet technology. The various internet-themed laws and treaties represent a concerted effort to balance the open, innovative potential of the Internet against its power as an aid to rights infringers.

But somewhere along the way, the newest thinking on international Internet regulation has taken a turn for the restrictive. The United States particularly, through the byzantine and complex Internet portions of the Digital Millennium Copyright Act (DMCA),[5] has greatly

---

[1] http://www.wikipedia.org/
[2] http://www.skype.com/intl/en-us/home/
[3] http://www.google.com/hostednews/afp/article/ALeqM5jVQgBFgqySdjDHb4I55eHKgl5hxg
[4] *See* Lessig, Lawrence. *The Future of Ideas.*
[5] 17 U.S.C. §§ 1201–1205

influenced this restrictive thinking. The newest negotiated multinational treaty, known as the Anti-Counterfeiting Trade Agreement, or ACTA, has an Internet chapter devoted to providing new mechanisms for maintaining these protectionism-centered concepts. The attitudes that gave birth to ACTA's Internet chapter are ferociously anti-innovative, in that they curtail both innovation in Internet technologies and in new forms of copyright law and enforcement.

In this article, I will discuss ACTA's treatment of both Internet service provider liability (including notice and takedown procedures and what is known as graduated response) and of copyright protection anti-circumvention measures. I will demonstrate how the formulation of these concepts in ACTA marks a clear manifestation of anti-innovative Internet law's influence on international negotiations.

II. Internet Service Provider Liability

Balanced against any measures protecting copyright and providing for enforcement of those rights are the limitations on liability for parties not directly engaged in those acts. While ACTA does provide a section creating 3rd party liability for those that aid in infringing, it also provides safe-harbor protection for internet service providers (ISPs).[6] The availability of these safe-harbors, however, is conditioned on certain action by the ISPs, specifically compliance with notice and takedown schemes and with creating certain types of "graduated response" enforcement provisions.

[6] ACTA Article 2.17: Enforcement procedures in the digital environment, §3. (Accessed at http://www.techdirt.com/articles/20100222/0215038248.shtml. This version is slightly outdated, as new versions have surfaced since, but for my discussion of attitudes on Internet regulation, this version provides adequate information.) (Hereinafter "ACTA")

A. Notice and Takedown

ACTA conditions protection for ISPs on implementing a notice and takedown procedure. The section defining and requiring this procedure is essentially a globalization of the United States' DMCA notice and takedown procedures. I will discuss the current global notice and takedown landscape and then compare it to what leaked drafts and official comments indicate about the direction notice and takedown is headed in ACTA, highlighting its free speech and policy innovation chilling effects.

i. Current Notice and Takedown Law

In the United States, the DMCA is the place to look for anti-circumvention. The US's approach to this type of scheme also provides the template on which most other countries based any similar provisions. The notice and takedown section seeks to define a procedure by which copyright holders can counter infringing content posted on the Internet. ISPs will have no liability for taking down material if they comply with the procedure defined in the DMCA.[7] In essence, when an Internet service provider is notified that one of their subscribers has posted infringing content, the service must remove that content. The person who initially posted it then has the chance to appeal this removal and have the content reinstated.

This procedure is the norm on the Internet in the United States, and it has been implemented in the European Union (EU) as well.[8] It is not the law in Canada, which commonly uses (and is likely implementing as law) a notice-and-notice system (i.e. notice of infringement begets notice to infringer).[9] WIPO has no provisions requiring it.

---

[7] 17 U.S.C. § 512(g)(1), 512(g)(2).
[8] *The European Union's Electronic Commerce Directive*, 2000/31/EC, Article 14.
[9] Geist, Michael. "ACTA Internet Chapter Leaks: Renegotiates WIPO, Sets 3 Strikes as Model." http://www.michaelgeist.ca/content/view/4808/125/

There is a large downside to this notice and takedown procedure. Parties seeking to protect their image or suppress content have used semi- or entirely-fraudulent takedown notices to have material they dislike removed from the Internet.[10] Further, websites hosting allegedly infringing content could suffer large amounts of collateral damage.[11] Notice and takedown provisions were also tied up in the story of the Church of Scientology's leaked documents, detailing possibly abusive procedures and bizarre doctrine.[12]

So notice and takedown is not a flawless system as it exists now. It's attempts to balance preserving copyright protection against the public's freedom of speech has tipped all too often against the public.

ii. What ACTA Mandates

ACTA essentially requires the adoption of notice-and-takedown procedures, modeled after the DMCA and the United States' recent bilateral agreements. ACTA specifically states, in one leaked version, that Internet service providers do not get any protections against liability for hosting infringing content unless they "expeditiously remov[e] or disabl[e] access to material or activity" that is allegedly infringing.[13] This adopts a procedure for notice and takedown strikingly similar to the DMCA's treatment of the same mechanism.

One thing that makes ACTA's version deficient in comparison to the DMCA version is the absence of an acknowledgement of fair use or fair dealing as a defense to takedown. The treaty

---

[10] *See, eg,* "The criticism that Ralph Lauren doesn't want you to see!" http://www.boingboing.net/2009/10/06/the-criticism-that-r.html (Ralph Lauren had criticism of their badly-photoshopped advertisements removed under the DMCA's takedown procedures)
[11] *See, eg*. "Another Reason To Worry About DMCA Takedowns: Collateral Damage." http://www.techdirt.com/articles/20100305/0430288433.shtml (discussing the takedown of a website as an illustration of the dangerous power of notice and takedown procedures).
[12] http://www.truthaboutscientology.com/dmca.html, "Mormons, Scientologists face uphill battle against Wikileaks." http://arstechnica.com/old/content/2008/05/mormons-scientologists-face-uphill-battle-against-wikileaks.ars
[13] ACTA §3(b)(II)

requires takedown of allegedly infringing material "in the absence of a legally sufficient response from the relevant subscriber of the online service provider indicating that the notice was the result of a mistake or misidentification."[14] Misidentification might mean content unidentified as a fair use. But unlike the DMCA's version of the system, no explicit protection remains for fair use and fair dealing. And fair use is very commonly identified, for example, as the defense to DMCA takedown notices on YouTube.[15]

ACTA also requires ISPs to disclose identities of parties infringing copyright after a mere request for this information. This would eliminate the protections for privacy and anonymity inherent in a procedure that requires a court order to get this information. Coupled with the notice and takedown procedures, this provision could encourage very invasive laws and policies in some nations.

The reality is that, even if ACTA pedals backward on this issue, it's clear that the treaty's purpose is to introduce a higher standard on foreign countries, one that is closer to the US's model for notice and takedown. This model, without any protection in ACTA for fair dealing, is therefore a sort of nuclear option in countries that do not already have a fair use exception. A work can be targeted and removed as infringing even if it only uses the original to comment upon it, in small portions, or in entirely reinvented ways.

B. Three Strikes

The "three strikes" principle seems to be relatively novel to the discussion surrounding ACTA itself. It might not remain in the final version, but it has influenced the discussion of Internet copyright enforcement surrounding the treaty.

---

[14] *Id.*

[15] http://googlepublicpolicy.blogspot.com/2010/04/content-id-and-fair-use.html

The "three strikes" model, also called graduated response, is a method of enforcement for ISPs against users caught infringing copyrights on their networks. Generally, "graduated response" would mean a method for responding directly to infringers, specifically by suspending or cutting off their access to the Internet. This kind of three-strikes procedure has been rejected often, and it's never been proposed as a part of United States law,[16] but the United States, according to an EU memo, was the party providing the most pressure to install such a provision.
It is unclear how much of this original "three strikes / graduated response" model remains in the current version of ACTA. The first hints of it surfaced in a draft proposed by the United States. The treaty's leaked text itself never actually included the provision, but a footnote proposed by the United States indicated that ISPs of all nations would be required / allowed to implement a policy "providing for the termination in appropriate circumstances of subscriptions and accounts in the service provider's system or network of repeat infringers."[17]

Since then, ACTA negotiators have claimed that the provision is gone from the treaty.[18] But even if the graduated response provisions or footnotes do not remain, they are obviously being discussed as one of the important reasons why ACTA must exist. The US is at least telling other nations that graduated response is legal and important, and such US pressure detracts from the freedom of other nations to experiment in more effective, less invasive methods of enforcing intellectual property rights.

III. Anit-Circumvention

Anti-circumvention requirements first came to international light under the WIPO Copyright Treaty, but they are most well-known in the united states as part of the DMCA. ACTA

[16] http://www.eff.org/deeplinks/2009/11/leaked-acta-internet-provisions-three-strikes-and-
[17] ACTA footnote 6.
[18] http://www.wired.com/threatlevel/2010/04/acta-treaty/

heightens global requirements for anti-circumvention law beyond where many participating nations already stand and beyond what WIPO required, chilling technological innovation in any country that enacts the provision as ACTA mandates it.

A. Current Practices

In 1996, the WIPO Copyright Treaty was enacted.[19] This treaty stated that member nations must provide protection and remedies "against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights."[20] The treaty also mandated "provid[ing] adequate and effective legal remedies against any person knowingly … remov[ing] or alter[ing] any electronic rights management information without authority..."[21] As a response, member nations had to install anti-circumvention provisions in their copyright acts.

Most notably, the United States implemented anti-circumvention rules as part of the DMCA. Under the DMCA, "no person shall circumvent a technological measure that effectively controls access to a work protected under [the copyright act]."[22] The section essentially criminalizes the circumvention of technological measures designed to protect copyrights. For instance, ripping a movie from a DVD would be circumvention of the encryption on that DVD. While there is an exception for home or personal copying of this kind, it is still illegal to sell or commercialize products that perform this kind of circumvention service.[23] The EU has also enacted some provisions on anti-circumvention.[24]

---

[19] *WIPO Copyright Treaty*, S. Treaty Doc. No. 105-17 (1997)
[20] *Id*. at Article 11.
[21] *Id.* at Article 12.
[22] 17 U.S.C. § 1201(a)(1)
[23] 17 U.S.C. § 1201(b)
[24] *European Union Directive on Anti-Circumvention*, 2001/29/EC.

As an example of how anti-circumvention law interacts with technological innovation, the debate over "jailbreaking" iPhones is one tied to anti-circumvention. Users want to be able to use free or open applications not directly provided by Apple on their iPhones, but the phones themselves include software locks that don't allow them to run unauthorized applications. So, some users have taken to removing these locks in a process called jailbreaking. This process has not been criminalized yet, but it provides a good example of the kinds of technologies that are threatened or limited by anti-circumvention provisions.[25]

B. What ACTA Mandates

Beyond what is required in the WIPO treaty, ACTA includes specific requirements for anti-circumvention law. The provisions in ACTA are not that surprising, requiring protection against circumvention and the selling of circumvention technologies.[26]

ACTA also requires that circumvention become criminal and civil offenses.[27] While such a provision might seem innocent, it makes it clear that, at least with respect to circumvention, ACTA seeks to supercede the substance of current law, i.e. it is not merely an enforcement treaty, as is often claimed by its proponents.

As to the form of the requirements, essentially, ACTA exports US law on the subject, but without the protection of the fair use exception. Additionally, while nations can still make exceptions to ACTA provisions, "so long as they do not significantly impair the adequacy of legal protection of those measures" or "the effectiveness of legal remedies for violations of those measures," the treaty does not even suggest an exception for innovators, educators, or any other fair use types of uses.

---

[25] http://www.eff.org/deeplinks/2009/02/apple-says-jailbreaking-illegal.
[26] ACTA §2,17(4)(a) and (b)
[27] ACTA §2.17(5)

This presents a large danger to those that wish to experiment and innovate with technologies. The lack of protection for innovators in this section is the strongest indicator for ACTA's indifference to the future of innovative technology. Further, the anti-circumvention provisions show an indifference to the ability of other nations to experiment with new ways of thinking about technological circumvention, ways that will help developing nations further hone their technologies and understand the technology their nation needs to grow.

IV. Conclusion

The concerns over ACTA's Internet chapter are obviously varied, and they are not centered in just one place. ACTA rewrites the law in a few countries and requires enforcement procedures never actually implemented in even the harshest copyright protection regimes. But the complaints all come down to two: the limiting of technological innovation and the thwarting of legal and policy innovation.

ACTA makes it extremely difficult for nations to allow their citizens to experiment with new technology. Anti-circumvention without a fair use exception spells immediate limitation on tinkerers and home innovators, the kinds of people who have helped the Internet progress as far as it has around the world.

But more importantly, ACTA limits the fundamental right of nations to try new legal methods of enforcement and policies on Internet regulation. The treaty essentially exports the United States' DMCA provisions to any member nations. But scholarship is divided on the sustainability and effectiveness of the DMCA. And even if the world agreed on the DMCA, it would still be necessary to allow each nation to craft a scheme that best fits with its national law.

Finally, the lack of any fair use provisions or protections in ACTA makes it a dangerous piece of law. It requires nations without protections for speech and civic participation to install

legislation that seems to rely on such protections. Such an act is akin to requiring all citizens to own pools in landlocked nations where no one knows how to swim; pool peddlers will get a boost, but citizens will be thrust into a situation where their fundamental rights are in severe danger.

ACTA can be an effective, important treaty, making strides to harmonize copyright protection with the freedom of the Internet. But until negotiators open the doors on comment and involvement, and until the United States backs down on demanding a global DMCA, the treaty will remain a danger to the innovative spirit that built so many nations and the Internet itself.