9-1-2010

ACTA's Abandoned Third-Party Liability Provisions and What They Mean for the Future

Michael R. Morris
University of Edinburgh, mrmorris@morris-morris.com

NAVIGATING THE ACTA SHOALS TO A FUTURE SAFE HARBOR: LIBRARY AND HOTSPOT INTERNET ACCESS LIABILITY IN A POST-ACTA UNIVERSE[1]

Michael R. Morris[2]

ABSTRACT

This white paper examines issues potentially created both by the expansion of third-party liability mandated by ACTA and the safe harbor provisions designed to provide some protection against that third-party liability.

[1] At the time this paper was researched and written, the July 1, 2010 draft of ACTA was the most recent draft of the text. Any references to "the most recent text" and related analysis refer to the July 1, 2010 draft. After this paper was submitted for publication, a new draft of ACTA was leaked on Aug. 25, 2010. This paper may be revised by the author to reflect changes made by the Aug. 25, 2010 draft text.

[2] Ph.D. Candidate, University of Edinburgh.

I. BACKGROUND

In the struggle against copyright infringement—including so-called "piracy"—internet service providers (ISPs) are easy targets for right holders and regulators. Attempts in both the United States and Europe have been made to determine and control the liability of ISPs, but the proposed Anti-Counterfeiting Trade Agreement (ACTA) threatens to upset the existing framework of ISP liability and impose significant new burdens on smaller providers: libraries, coffee shops and other non-traditional service providers. This paper focuses on the issues of third party liability and potential problems with ACTA safe harbor compliance—*i.e.*, affirmative duties to protect copyrighted material from infringement—of coffee shops and libraries that provide internet access through hotspots or computer rental. These businesses' core focus is not the provision of internet services, which are provided as a service or inducement to patrons, so this paper refers to them as ancillary service providers (ASPs). While it is unclear how many ASPs exist, JiWire counted 299,291 hotspots worldwide as of 7 June 2010.[3] Because of the nature of the internet, ISPs are theoretically responsible as third parties for the infringements of their users. Third party liability allows for suits, damages, and liability against parties that have not themselves violated any laws. Third party liability is imposed in the United States through the doctrines of vicarious liability and contributory or comparative liability.[4] Ever since *Sony Corp. v. Universal City Studios*[5] (aka *Betamax*), American courts have been struggling with the problem of apportioning liability for copyright infringement in an era of

[3] JiWire is an online registry of free and paid international Wi-Fi locations. http://v4.jiwire.com/search-hotspot-locations.htm.

[4] *Sony Corp. v. Universal City Studios*, 464 U.S. 417, 434–435 (1984). In the contributory liability scenario, a party either materially contributes to copyright infringement or induces the copyright infringement. *Perfect 10 v. Visa Int'l Serv. Ass'n*, 494 F.3d 788 (9th Cir. 2007). This paper focuses mainly on vicarious liability and will not address contributory liability other than incidentally.

[5] 464 U.S. 417 (1984).

constant technological innovation.[6] *Betamax* established the principle that producers of products—VCRs in that case—could not be held liable for secondary infringement, even where infringement had occurred, if the product had substantial non-infringing uses.[7] In the internet era, in *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*,[8] the Supreme Court of the United States set forth, albeit in a fractured fashion, the current rule on inducement of copyright infringement, holding that "one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties."[9]

In the United States, there are specific statutes governing third party, or secondary, liability with regard to trademarks and patents, but not for copyright, in which area the doctrine of secondary liability has been developed by case law, especially *Betamax* and *Grokster*, discussed briefly above.[10] In an attempt to clarify liability for ISPs, however, statutes such as the Digital Millennium Copyright Act (DMCA) have been passed that provide "safe harbors."[11] Safe harbor provisions provide guidelines for ISPs to follow and provide immunity from primary copyright liability. The DMCA provides safe harbors for four different aspects of service: transitory network communications; system caching; information storage, and information location tools. To qualify for safe harbor, a service provider must adopt and implement policies to terminate the accounts of repeat infringers and must allow and not interfere with standard procedures used by copyright owners to protect their works. For the information storage and information location tools safe harbors, the service provider must not receive a financial benefit from the infringing activity.[12]

---

[6] To be sure, every technological development has created this problem, but the development of consumer-level technologies that allow cheap and easy copying of copyrighted materials has vastly accelerated and expanded the problem.

[7] 464 U.S. at 491.

[8] 545 U.S. 913 (2005).

[9] *Id.* at 919.

[10] Congress has not been inactive in legislatively addressing the liability of ISPs for speech posted on the internet, passing such laws as the Communications Decency Act, § 230 of which has been interpreted to provide immunity to ISPs from torts committed by users of a website or online forum. *See Zeran v. America Online,* 129 F.3d 327 (4th Cir. 1997). This doctrine has not been universally adopted, and it will pose a problem for ACTA harmonization.

[11] 17 U.S.C. §512.

[12] Service providers need not derive a direct financial benefit from the infringing activity. In *A&M Records, Inc. v. Napster*, 239 F.3d 1004 (9th Cir. 2001), the court held that merely drawing an increased number of visitors to a venue could be an adequate benefit. This holding certainly suggests that a court might find that internet access is a draw to customers or patrons, thus leading to increased funding or business. This very

Additionally, with regard to the last three safe harbors, the service provider must implement a set of "notice and take down" procedures.

Europe has adopted a similar system in the form of the E-Commerce Directive, which provides exemptions from liability for service providers operating as mere conduits or providing only temporary caching.[13] The Directive currently bars member states from imposing a general obligation to monitor content, but does have a notice and takedown requirement for immunity from liability where the service provider provides any hosting services.[14]

While most colleges and universities have put such policies in place and have been concerned about copyright infringement since the creation of the photocopier (and the DMCA has special provisions for non-profit educational institutions[15]), small businesses and other ASPs may either be unaware of the relevant provisions or have made a business decision that the cost of compliance outweighs the benefits of protection. Businesses can choose not to comply because the safe harbors are voluntary[16]—no business has to incur the expense or go through the procedures of compliance. Consider, for example, the notices regarding copyright infringement seen in every library, if not on every copy machine in them. By contrast, a copier in the business center of a hotel will not have such notices as it makes no business sense to go to that expense. Informed decisions can be made by would-be ASPs because the scope of liability is relatively clear, as is the scope of the protections offered by the safe harbor provisions. (Granted, there is still debate about the interpretation of *Grokster*.) Neither is the case with ACTA. This uncertainty is particularly troubling for libraries and academic institutions whose students and patrons often engage in the creation of content through sites like Facebook. In a post-ACTA world, the burden to police such activity might well fall on the library. Rather than assume such a burden, many institutions might find themselves banning access to entire categories of sites, both social and, in the case of blogs, academic.

---

argument of drawing customers was used by Viacom in its recent litigation against YouTube.

[13] Directive 2000/31, para. 43, 2000 O.J. (L 178) 6 (EC).

[14] *Id.* art. 21, para. 2.

[15] 17 U.S.C. § 1201(d) (2006).

[16] Judge Posner, in *In re Aimster Copyright Litigation,* 334 F.3d 643 (7th Cir. 2003), held that service providers must have mechanisms in place to monitor their systems for infringing activity and terminate the accounts of repeat infringers to qualify for safe harbor protection. This decision is important both for the holding that service providers cannot maintain a blind eye to infringing activity and for the DMCA definition of "service provider," which designation was to be broadly interpreted.

The exact form of the ACTA safe harbor provisions is unknown, as the released text offers multiple options and proposals that appear to have at least some relationship to the DMCA and E-Commerce Directive safe harbor provisions, and uses a very broad definition of third party liability. ACTA Article 2.18(3) deals specifically with third party liability for copyright infringement. Two footnotes are of interest. Taking them out of order for analytic purposes, ISPs will clearly meet the definition of online service provider offered in footnote 48 as ISPs provide connections for digital online communications. [17] Footnote 46 defines third party liability as "liability for any person who authorizes for a direct financial benefit, induces through or by conduct directed to promoting infringement, or knowingly and materially aids any act of copyright or related rights infringement by another." [18]

This language would dramatically expand third party liability both in the United States and around the world, not least because not every nation has a doctrine of third party liability for copyright infringement. In the United States, it would go far beyond traditional American definitions of secondary liability especially as footnote 46 goes on to list fair use as a "legitimate interest of the right holder" rather than an exception or limitation to copyright.[19] While final language has not been settled, it appears that the ACTA safe harbor language would require significantly greater active monitoring for copyright infringement. Among the proposals are requirements that the service provider remove infringing material of its own volition, rather than waiting for a take-down notice; that service providers provide right holders with information on the identity of a subscriber believed by the right holder to be infringing, and service providers enter into a "mutually supportive" relationship with right holders. Harmonizing ACTA requirements to block or prevent access of serial infringers with European laws on privacy will be difficult and expensive for all service providers, including ASPs.[20]

---

[17] "For purposes of this Article, online service provider and provider mean a provider of online services or network access, or the operators of facilities therefore, and includes an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received." Anti-Counterfeiting Trade Agreement Informal Predecisional/Deliberative Draft: July 1, 2010, art. 2.18(3), PIJIP IP ENFORCEMENT DATABASE, http://sites.google.com/site/iipenforcement/acta (follow "Full Leaked Text Dated July 1, 2010" hyperlink) [hereinafter ACTA Draft – July 1, 2010].

[18] *Id.*, art 2.18, ¶ 2.

[19] *Id.*

[20] In particular, *Productores de Música de España (Promusicae) v. Telefónica de España S.A.U.*, European Court of Justice (Grand Chamber), Case C-275/06, 2008, held

The proposed language may be at odds with current law but is consistent with pressure being brought by right holders, who around the world are bringing cases seeking to hold ISPs responsible for the use to which their users put their connections. In the Australian case of *Roadshow Films v. iiNet*, a consortium of film studios and their licensees unsuccessfully sued the country's third largest ISP, iiNet, for copyright infringement.[21] In *Roadshow*, the film studios alleged that the ISP permitted its users to access copyright material via a BitTorrent network, even after the studios had notified the ISP and asked that the infringing user's accounts be terminated. The Court ruled in favor of iiNet, finding that iiNet did not authorize the infringement of copyright by iiNet users by merely providing internet access as some other tool—a website or BitTorrent site—was needed to infringe copyright, and Australian law imposed no affirmative obligation on any person to protect the copyright of another. Likewise, governments are taking an increasingly aggressive stance toward ISPs, as in the recent case in Italy in which Italian prosecutors filed criminal charges against Google executives based on the content of a video showing the bullying of disabled schoolchildren.[22] Even though Google quickly took down the video and cooperated with authorities—which led to the successful prosecution of the uploader—three executives were convicted of privacy code violations. Most recently, the United Kingdom adopted the Digital Economy Act 2010 which requires ISPs to provide right holders with a copyright infringement list, block access to sites that allow substantial infringement, and disconnect repeat infringers.[23]

While it may be understandable that a library offering wi-fi and wired connections might be considered an ASP, there is no floor on the number of users or the nature of the provided connection. Considering that Germany's highest court recently ruled that internet users must protect their private wireless networks with a password to prevent copyright infringement,[24] there is certainly precedent for the floor on ASPs to be very low indeed.

---

that European law does not require the disclosure of user identification in civil cases, but that member states could seek to impose such requirements.

[21] *Roadshow Films Propriety Lt.d v iiNet Limited (No. 3)* (2010) FCA 24 (Austl.).

[22] *See* David Meyer, *Italy Convicts Google Execs over Bullying Video*, ZDNET UK (Feb. 24, 2010, 12:49 PM), http://www.zdnet.co.uk/news/networking/2010/02/24/italy-convicts-google-execs-over-bullying-video-40052438/.

[23] Digital Economy Act, 2010, c. 24, §§ 4,7,11.

[24] *See* Kristen Grieshaber, *German Court Orders Wireless Passwords for All: Users Can Be Fined If a Third Party Takes Advantage of an Open Connection*, MSNBC.COM (May 12, 2010, 10:55 AM), http://www.msnbc.msn.com/id/37107291/ns/technology_and_science-security/.

ACTA seems focused on protecting the interests of right holders without providing the kinds of protections and exemptions that have been developed in the United States. ACTA contains no parallel to the immunity doctrine provided by the Communications Decency Act[25] or the "substantially non-infringing" use doctrine of *Betamax*. Instead, ACTA simply demands the imposition of third party liability for conduct promoting infringement. Furthermore, by requiring ISPs to operate as "copyright police" in return for safe harbor protection, ACTA essentially shifts the expensive burden of copyright protection from the right holder to the service provider. Moreover, it is completely unclear whether a service that has fully complied with the safe harbor provisions would be exempt from the Article 2 mandate on injunctive relief, thereby potentially increasing legal costs for all service providers, not just ASPs.

II. ASP CONCERNS

For ASPs that provide connections to transient users, identifying infringing users—as the user would, by definition, no longer be at that address—is a problem. Consider the example of a library that provides computers for the use of patrons. A patron—one of many using the computer that day—could log on and download copyrighted material; transfer the material to a flash drive or other storage device, and then leave. Even worse is the problem of identifying users of wireless networks. Even assuming that technology exists for creating a globally unique identifier for a user of a laptop or mobile web device, it does not follow that an ASP would be able to easily or cheaply use that information to block repeat infringers.

Given that the ASP will most often be the customer of a larger provider, it is in the position of *being* both the infringing user from the point of view of the larger ISP, and responsible for stopping the infringing activity from the point of view of the rights holder. Thus, the ASP might face disconnection from the internet by its provider at the same time it was facing demands from the right holder to stop the infringement. This dilemma was identified as a particular concern by groups opposing the Digital Economy Bill in the United Kingdom.

Even if an ASP were able to identify a repeat infringer, there are serious implications for both privacy and, where the ASP has charged for internet services, contract. European laws on privacy are different and sometimes stricter than United States laws, and it is difficult to see how universally

[25] 47 U.S.C. §230 (2006).

ACTA-compliant laws could be drafted. Where a patron has paid for access to the internet, the ASP puts itself at risk of suit if it denies access to the user on infringement grounds, especially if such infringement were later shown not to have occurred. While relatively few users would file suit over a few dollars lost on a connection falsely terminated, it is not difficult to envision class actions brought if such behavior were to become widespread.

Many ASPs do not just provide a conduit to the internet, but also have a portal page from which a user might link to items of local interest and, after the click to acknowledge terms and conditions, access the internet. Under ACTA, the ASP might be required to police stored data or links for copyright infringement. For a local hotel or restaurant trying to provide access to local points of interest or to promote tourism, this would be an unwelcome and perhaps unsustainable burden.

One other area of concern should be noted, even though it does not present issues of third party liability. Article 2.14 (a) of the ACTA draft provides for criminal liability for willful copyright piracy on a commercial scale, even where the infringement is not directly or indirectly motivated by financial gain. It is far too easy to foresee an ASP being targeted for either the peer-to-peer file swapping of its patrons or for large numbers of leaked documents posted by an activist group (especially if the ASP allowed the creation of forums or groups).

III. POSSIBLE SOLUTIONS

There are several possible solutions to ASPs' concerns about ACTA. The first, of course, would be to reject ACTA in its entirety. For all ISPs, an exclusion from liability for providing transitory network communications would best reflect the reality that ISPs have no way of inspecting internet traffic in real time to ensure that no copyright infringement is taking place. Assuming, however, that some form of ACTA will be negotiated and accepted, the simplest remedy for the concerns of ASPs would be to modify the definition of service provider. A number of possible options exist, although it would be difficult to construct a bright-line rule. At a minimum, the definition should exclude businesses that offer internet access only as adjuncts to their primary businesses or those which contract with providers for hotspot service for their customers. Such a definition might not aid libraries, which are increasingly net-centric, so a blanket exclusion of libraries would also be appropriate.

However, excluding ASPs from the ACTA definition of service provider only solves half the problem, as it would not only strip ASPs of the affirmative duties imposed by ACTA (a welcome modification), but also of

the safe harbor protections of the DMCA, an unwelcome change. Perhaps the best compromise, then, would be to create a special class of service providers tailored to the needs of ASPs. Such a policy would:

• apply only to service providers which provide on-site access for limited periods of time;

• bar liability for acting as a mere conduit or providing caching services, without imposing any obligation on the ASP to take any affirmative step to protect the interest of right holders;

• bar criminal liability for ASPs for commercial-scale infringement by users of the ASP connection;

• bar third party liability for people with a home wi-fi system;

• provide that ASP connections cannot be terminated by their providers on the basis of infringing use by ASP patrons, absent proof that the ASP knowingly fosters such activity;

• exclude ASPs from liability for injunctive relief, absent proof that the ASP has actual knowledge that its service is being used to infringe copyright,[26] and

• bar third party liability for ASPs for user-created content that contains infringing material.

In addition, negotiators may wish to consider some sort of intermediate status or contractual assumption of liability for ASPs offering internet access through hotspots operated by other ISPs, such as T-Mobile, AT&T. Where the coffee shop internet access is being provided by a separate company, the ASP may not have the ability to exercise the control over the connection necessary to comply with ACTA safe harbor provisions. This will be a particularly difficult problem to resolve, as several different business models are used by hotspot providers, ranging from turnkey systems in which the ASP has no control, and the hotspot uses a separate connection from the business' operating connection to systems in which the ASP uses its own connection and simply pays one upfront cost for equipment and software.

ACTA may not turn out to be the freedom-eating, copyright excreting monster that it was portrayed to be in the blogosphere, but the draft version released thus far raises serious concerns for small business and library

[26] Such language is found, for example, in the United Kingdom's Copyright, Design and Patents Act 1988.

hotspot providers. As presently drafted, ACTA would both expose such entities to significant liability, including possible criminal liability, and provide them with safe harbors far too expensive and difficult for them to navigate. Policy makers must remember that the internet is not only comprised of Google, AT&T and British Telecom, but also small coffee shops like Elephants and Bagels that have a single wireless router tucked under the counter with a sign that says "please don't stay on the internet all day." A regulatory system that fails to address the needs and capacities of small business is likely to have a chilling effect on access to the internet and electronic commerce. After all, right holders do not want to shut off access to iTunes in the process of trying to stop illegal downloading.