ACTA ON LIFE SUPPORT: WHY THE ANTI-COUNTERFEITING TRADE AGREEMENT IS FAILING AND HOW FUTURE INTELLECTUAL PROPERTY TREATIES MIGHT AVOID A SIMILAR FATE

INTRODUCTION

The Anti-Counterfeiting Trade Agreement ("ACTA" or "Agreement") is an international intellectual property treaty that provides for new international minimum standards for criminal and civil enforcement of intellectual property rights.[1] The categories of subject matter protected by the agreement are borrowed from the Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS"),[2] and ACTA expands upon the limited criminal enforcement standards present in TRIPS.[3]

ACTA is an agreement created outside the auspices of multilateral organizations[4] and has been fraught with controversy since its initial talks

1. A signing ceremony was held on October 1, 2011 in Tokyo, Japan, at which Australia, Canada, Japan, Korea, Morocco, New Zealand, Singapore, and the United States signed the Agreement. *Joint Press Statement of the Anti-Counterfeiting Trade Agreement Negotiating Parties*, OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE (Oct. 2011), *available at* http://www.ustr.gov/about-us/press-office/press-releases/2011/october/joint-press-statement-anti-counterfeiting-trade-ag. While not signing it, the European Union, Mexico, and Switzerland "confirmed their continuing strong support for and preparations to sign the Agreement as soon as practicable." *Id.* Twenty-two EU member nations have since signed the Agreement, though it has not been ratified by the European Parliament, arguably because of public backlash against the Agreement. Dave Lee, *Acta Protests: Thousands Take to the Streets Across Europe*, BBC NEWS (Feb. 11, 2012, 1:57 PM), *available at* http://www.bbc.co.uk/news/technology-16999497. The Agreement will enter into force once six member nations enter instruments of "ratification, acceptance or approval." Anti-Counterfeiting Trade Agreement art. 40(1), *opened for signature* Oct. 1, 2011 [hereinafter ACTA or Agreement], *available at* http://www.mofa.go.jp/policy/economy/i_property/pdfs/acta1105_en.pdf. The other parties to the Agreement are Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden. *Id.* art. 39 n.17.

2. *Id.* art. 5(h). The categories of intellectual property protected under TRIPS are copyrights, trademarks, geographical indications, industrial designs, patents, layout-designs of integrated circuits, and protection of undisclosed information. *See* Agreement on Trade-Related Aspects of Intellectual Property Rights Part II, Apr. 15, 1994, 1869 U.N.T.S. 299 [hereinafter TRIPS, TRIPS Agreement, TRIPS Part II or TRIPS Agreement Part II].

3. TRIPS provides only that "[m]embers shall provide for criminal procedures and penalties to be applied at least in cases of willful trademark counterfeiting or copyright piracy on a commercial scale," and allows for imprisonment and fines commensurate with the offense. TRIPS Agreement, *supra* note 2, art. 61.

4. Unlike many other international IP treaties, ACTA was conceived of and drafted independent of multilateral organizations such as the World Trade Organization ("WTO") or the World Intellectual Property Organization ("WIPO"). *See* Eddan Katz & Gwen Hinze, *The Impact of the Anti-Counterfeiting Trade Agreement on the Knowledge Economy: The Accountability of the Office of the*

in 2006, with criticism ranging from its negotiations lacking transparency to its very existence merely being an initiative by rights holders to increase the international power of their intellectual property rights.[5] Events in 2012 have created significant uncertainty as to the likelihood of the agreement coming into effect; the European Union parliament affirmatively declined to ratify it,[6] and several European nations have refused to ratify ACTA in the wake of large protests.[7]

This Note is concerned with one particular criticism of ACTA: that despite its title and provisions for counterfeit goods, it is primarily a copyright treaty designed to respond to growing concerns of rights holders with respect to digital copyright infringement.[8] Whether or not this criticism is valid, ACTA does contain several provisions relating to copyright infringement and piracy, both physical and digital, which are not present in prior IP treaties.[9] And although the future of ACTA is far from certain (and likely far from bright), its goals within this sphere of

---

U.S. Trade Representative for the Creation of IP Enforcement Norms Through Executive Trade Agreements, 35 YALE J. INT'L L. ONLINE 24, 26 (2009), http://www.yjil.org/docs/pub/o-35-katz-hinze-ACTA-on-knowledge-economy.pdf (arguing that parties to ACTA chose to negotiate apart from these organizations because they lack enforcement power).

5. *See* Charles McManis, *The Proposed Anti-Counterfeiting Trade Agreement (ACTA): Two Tales of a Treaty*, 46 HOUS. L. REV. 1235 (2009). The negotiations for the Agreement were carried out behind "closed doors" while industry representatives were provided with information not available to the general public. *Id*. at 1236. Even more conspicuously, the Office of the U.S. Trade Representative ("USTR") in 2009 denied a Freedom of Information Act request for documents related to the Agreement's negotiations on the claim that they were state secrets. *Id*. at 1238; *see also* Grant Gross, *Obama Administration Says Treaty Text Is State Secret*, PC WORLD (Mar. 13, 2009), http://www.pcworld.com/article/161234/article.html (citing to a letter from the USTR stating that "information in ACTA . . . is 'properly classified in the interest of national security'").

6. The EU parliament rejected ACTA by a plenary vote of 478–39 on July 4, 2012. *European Parliament Rejects ACTA*, EUR. PARLIAMENT (July 2–5, 2012), http://www.europarl.europa.eu/news/en/headlines/content/20120618FCS47114/9/html/European-Parliament-rejects-ACTA. After the parliament's rejection of the agreement, the European Commission suggested that it would seek an opinion of the EU Court of Justice on the compatibility of ACTA with EU law to make it seem more palatable to its detractors, but by the end of 2012 the EC withdrew its request for an opinion. *See* Jack Phillips, *'End of the Road' for ACTA in Europe*, THE EPOCH TIMES (Dec. 20, 2012), *available at* http://www.theepochtimes.com/n2/world/327064-327064.html.

7. *See Acta Approval Stalled by European Commission*, THE GUARDIAN (Feb. 22, 2012, 11:24 AM), *available at* http://www.guardian.co.uk/technology/2012/feb/22/acta-stalled-european-commission (reporting that Bulgaria, the Netherlands, Poland, and Germany have refused to ratify ACTA); *see also* Charles Arthur, *Acta Goes Too Far, Says MEP*, THE GUARDIAN (Feb. 1, 2012, 9:39 AM), *available at* http://www.guardian.co.uk/technology/2012/feb/01/acta-goes-too-far-kader-arif (reporting that the European Parliament's lead negotiator for ACTA resigned from his position over concerns about the agreement).

8. *See* Margot E. Kaminski, *An Overview and The Evolution Of The Anti-Counterfeiting Trade Agreement*, 21 ALB. L.J. SCI. & TECH. 385 (2011), *available at* http://www.albanylawjournal.org/Documents/Articles/21.3.385-Kaminski.pdf. Kaminski asserts that "ACTA is primarily a copyright treaty, masquerading as a treaty that addresses dangerous medicines and defective imports." *Id*. at 386–87.

9. *See* TRIPS Part II, *supra* note 2.

intellectual property will not be interred along with it. Though the agreement may die, an autopsy could provide valuable information on trends in the development of IP treaties and how future treaties might avoid a similar fate.

This Note argues that the digital infringement provisions of ACTA are the result of a progression of international IP treaties,[10] and that its specific provisions regarding Digital Rights Management ("DRM")[11] and digital infringement are both strongly influenced by the U.S. Digital Millennium Copyright Act ("DMCA")[12] and a reaction to legal battles involving new technology used to facilitate digital copyright infringement. This Note further argues that, despite the continuing rise in this infringement, ACTA's provisions go too far in protecting the interests of rights holders at the expense of internet service providers ("ISPs"),[13] Internet content providers ("ICPs"),[14] and internet users. Specifically, the Agreement should either have reduced standards of liability for these groups or, in the alternative, the Agreement should provide explicit defenses and exceptions for liability, and should provide specific guidelines on implementing concepts of secondary liability for countries that do not have well-established legal doctrine regarding secondary liability.

Part I begins with a comparison between ACTA and multiple IP treaties and statutes that predated its creation in regards to digital copyright infringement. Part I examines the current state of the legal issues regarding digital piracy with which ACTA is concerned, specifically by discussing court cases concerning liability for ISPs of their users'

10. The specific treaties discussed are TRIPS and the World Intellectual Property Organization Copyright Treaty ("WIPO Treaty" or "Treaty"). While several bilateral treaties have been created subsequent to these treaties, TRIPS and the WIPO Treaty provide an indication of the development of international standards relevant to a discussion of ACTA. *See* Peter Drahos, *BITs and BIPs: Bilateralism in Intellectual Property*, 4 J. WORLD INTELL. PROP. 791, 792–807 (2001) (discussing the development of bilateral trade agreements with IP provisions more stringent than those found in TRIPS).

11. Also known as Electronic Rights Management ("ERM"), these are measures that can be taken on digital products (such as software and computer files that contain copyrighted works) by which a rights holder can prevent certain uses of these products (restricting the ability to make copies of music files on a computer is a common form of DRM). The use of DRM is controversial, as its proponents claim it is necessary to protect the interests of right holders and prevent infringement, while its critics claim that DRM does little to prevent infringement and prevents legal uses of copyrighted works. For a discussion of this tension between rights holders and users, see Timothy K. Armstrong, *Digital Rights Management and the Process of Fair Use*, 20 HARV. J.L. & TECH. 49 (2006).

12. 17 U.S.C. §§ 512, 1201 (1999).

13. ISPs are subscription services that provide internet access to users. *See, e.g.*, *id.* § 512(k)(1).

14. For purposes of this note, ICPs are websites that host or link to content that is frequently the subject of copyright infringement litigation.

copyright infringement. Part II continues with a discussion of why ACTA is the logical outgrowth of the treaties and DMCA. Part III then posits the argument that the Agreement is too harsh in its minimum international enforcement standards. To support this latter contention, this Note will focus on the lack of exceptions and defenses to infringement in ACTA and how its provisions may allow for states to enact draconian anti-pirating laws that might cut off alleged infringers from the internet. Finally, in Part IV, this Note will discuss what a better and more equitable version of ACTA might look like and the types of limitations that future ACTA-like treaties should incorporate to strike a better balance between IP holders and users.

I. THE LEGAL BACKGROUND OF ACTA

A. International Treaties and the DMCA

There are four aspects of ACTA that are relevant to the enforcement of intellectual property rights in the digital environment: digital copyright infringement, DRM circumvention, minimum standards for liability,[15] and disclosure of personal information.[16] It is interesting, then, that TRIPS spends very little time on these issues.

Being a product of the mid-90s, TRIPS was not concerned with many of the technological innovations that would form the basis for modern digital copyright infringement. It does, however, offer the groundwork for a discussion of privacy rights in cases of copyright infringement. TRIPS allows member states to require an infringer to disclose the identity of third persons related to instances of infringement.[17] In the realm of civil enforcement, TRIPS provides for provisional measures that can be adopted *inaudita altera parte* (without the other party present), so long as notice is given to the other party.[18] TRIPS also provides for exceptions to

15. *See* ACTA, *supra* note 1, art. 27(7).

16. *See id*. arts. 22, 27(4).

17. TRIPS provides that member states may require infringers "to inform the right holder of the identity of third persons involved in the production and distribution of the infringing goods or services and of their channels of distribution." TRIPS art. 47. This article also provides that member states may not grant this authority if doing so "would be out of proportion to the seriousness of the infringement." *Id.* While this is the opposite of a situation in which an ISP (a third party) is compelled to provide the identity of an infringer, the circumstances are not altogether different, and this language could conceivably lay the groundwork for later law and treaties that compel ISPs to provide the identities of alleged infringers.

18. TRIPS requires members to give judicial authorities the ability to order provisional measures "to prevent an infringement of any intellectual property right from occurring" and "to preserve relevant evidence in regard to the alleged infringement." *Id*. art. 50(1)(a)–(b). These provisional

the exclusive rights of rights holders, but only in broad language that favors the authors of copyrighted works.[19]

The World Intellectual Property Organization Copyright Treaty ("WIPO Treaty" or "Treaty"), created two years after TRIPS, fills some of the holes in the latter Agreement concerning computers and the internet. Specifically, the WIPO Treaty introduces provisions obligating member states to create legal remedies for DRM circumvention[20] and defining actionable circumstances of circumvention.[21] It also introduces an explicit right of communication to the public, which could be of legal relevance to Internet streaming sites, even if the WIPO Treaty may not have contemplated streaming technology.[22] Unfortunately, the Treaty's text offers little in the way of enforcement guidelines[23] or limitations on the new rights it creates.[24]

---

measures can be ordered in the absence of the party against whom the measures are taken, *id*. art. 50(2), but require that "the parties affected shall be given notice, without delay after the execution of the measures at the latest." *Id*. art. 50(4).

19. TRIPS provides that "[m]embers shall confine limitations or exceptions to exclusive rights to certain special cases which do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the right holder." *Id.* art. 13.

20. The WIPO Treaty obligates parties to:

> provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.

World Intellectual Property Organization Copyright Treaty art. 11, Dec. 20, 1996, 36 I.L.M. 65 [hereinafter WIPO Treaty or Treaty].

21. The Treaty requires members to create legal remedies against those who "remove or alter any electronic rights management information without authority" or "distribute . . . or communicate to the public . . . works or copies of works knowing that electronic rights management information has been removed or altered without authority." *Id.* art. 12(1)(a)–(b).

22. The Treaty gives copyright holders:

> the exclusive right of authorizing any communication to the public of their works . . . including the making available to the public of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them.

Id. art. 8.

23. Member states are only obligated to "ensure that enforcement procedures are available under their law . . . including expeditious remedies to prevent infringements and remedies which constitute a deterrent to further infringements." *Id.* art. 14(2).

24. The Treaty states:

> [c]ontracting Parties may . . . provide for limitations of or exceptions to the rights granted to authors . . . under this Treaty in certain special cases that do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the author.

Id. art. 10. This limitations language is essentially the same as that used in TRIPS that favors rights holders. This language becomes troublesome in regards to DRM, because restrictions placed on copyrighted works via DRM, such as copy protection, can prevent consumers from making fair uses of a given work, assuming that applicable law defines what a fair use is. Arguably, the use of DRM

As the U.S. statutory enactment of the WIPO Treaty, the DMCA is concerned with much the same subject matter as the Treaty. Its provisions on DRM circumvention are not considerably more expansive than those in the Treaty; they make it illegal to circumvent DRM[25] or, borrowing the "staple article of commerce" doctrine in patent law,[26] to traffic in devices that primarily contribute to circumvention.[27] This section of the DMCA also provides for fair use and other exceptions to a claim of infringement via circumvention.[28]

The more important section of the DMCA, insofar as it relates to how ACTA changes international IP law, is § 512, which deals with limitations of liability for ISPs and subpoena powers to obtain the identities of alleged infringers. Section 512 strikes a bargain with ISPs in which they are given "safe harbor," in certain circumstances, from liability for infringement claims that stem from certain conduct.[29] In exchange for this protection, ISPs agree to, when possible, remove infringing content and disclose identifying information of alleged infringers[30] when a right holder has provided a legally sufficient claim of infringement.[31]

---

changes what is a "normal exploitation of [a] work," and thus narrows what can be legally recognized as a fair use. *Id*.

25. 17 U.S.C. § 1201(a)(1)(A) (1999).

26. The Patent Act offers the foundation for secondary liability found in the Digital Millennium Copyright Act ("DMCA"). It provides that:

> [w]hoever offers to sell or sells . . . a component of a patented machine . . . or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial noninfringing use, shall be liable as a contributory infringer.

35 U.S.C. § 271(c) (2010).

27. The DMCA provides that:

> [n]o person shall . . . traffic in any technology, product, service, device, component, or part thereof, that—(A) is primarily designed or produced for the purpose of circumventing a technological measure . . . ; (B) has only limited commercially significant purpose or use other than to circumvent a technological measure . . . ; or (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure . . . .

17 U.S.C. § 1201(a)(2) (1999).

28. The DMCA provides that "[n]othing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use." *Id.* § 1201(c)(1).

29. The safe harbor provisions apply to situations in which ISPSs transmit, cache, store, or link to infringing material, subject to numerous qualifications. *Id*. § 512(a)–(d).

30. *Id.* §§ 512(c)(1)(iii), 512(h)(5).

31. In addition to filing a request for a proposed subpoena and giving a sworn declaration, the right holder must identify the copyrighted work claimed to have been infringed and provide "[i]dentification of the material that is claimed to be infringing . . . and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material." *Id.* § 512(h) (citing § 512(c)(3)(A)(iii)).

B. Litigation Relevant to ACTA's Provisions

To see ACTA's provisions in context, especially those regarding liability of ISPs, it is important to understand how secondary liability for digital copyright infringement has played out in litigation. Courts, both in the U.S. and abroad, have limited liability for ISPs and ICPs to instances in which they have contributed to or induced the infringing activities of users to impose liability, though precisely what conduct leads to this liability can be uncertain.

Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.[32] provides a template for secondary liability of ISPs and ICPs under U.S. law. Defendants were two companies that distributed software which allowed users to engage in P2P file sharing.[33] Billions of files were shared amongst users on a monthly basis, the majority of which defendants knew were copyrighted works.[34] The defendants' involvement went beyond mere knowledge of infringement, however. Both companies actively sought to distribute their software to prior users of the notorious file-sharing website Napster after it had been found liable for its users' copyright infringement,[35] and advertised the availability of copyrighted works through their services.[36] While the general rule for secondary liability for copyright infringement precludes fault if a distributed product is capable of significant lawful purposes,[37] the affirmative steps taken by Grokster and Streamcast were sufficient for a finding of liability under the theory of inducing copyright infringement.[38]

---

32. 545 U.S. 913 (2005).

33. The two defendant companies were Grokster, Ltd. and Streamcast Networks, Inc. *Id.* at 920.

34. The Supreme Court found that "it is uncontested that [defendants] are aware that users employ their software primarily to download copyrighted files." *Id.* at 923.

35. *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

36. Streamcast developed a program called "OpenNap" after suit was brought against Napster, which was designed to attract Napster users in the event that the site was shut down. *Id*. at 924–25. Grokster inserted codes into its website that redirected people searching for "Napster" to its site. *Id*. at 925. Both services distributed promotional material to their users informing them of the ability to use these services to download popular copyrighted material. *Id.* at 926. Also, the Court found that the business model for both services was relevant to a finding of liability. The revenues of Grokster and Streamcast came entirely from selling advertising space, and the monetary value of this advertising space rose in proportion with the volume of traffic to their websites. *Id.*

37. *See* Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417, 456 (1984) (holding that VCR distributor's awareness that such devices could be used for infringing purposes was not sufficient for a finding of secondary liability when knowledge of specific instances of infringement was absent and the devices could be used for significant non-infringing purposes). The Court in *Grokster* specifically found that "mere knowledge of infringing potential or of actual infringing uses would not be enough here to subject a distributor to liability." *Grokster*, 545 U.S. at 937.

38. The Court held 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

The Swedish litigation against the owners of the infamous file-sharing site The Pirate Bay[39] illustrates that the rationale for finding secondary copyright infringement liability for ICPs in Europe is similar to that in the U.S.[40] The Pirate Bay is a website that hosts "torrents," which facilitate the downloading of files over a P2P network.[41] Individual users of The Pirate Bay had used the website to infringe copyright in multiple works,[42] and the Swedish government brought a criminal action against the owners of The Pirate Bay.[43] Like in *Grokster*, the defendants were aware that a large number of their users were engaged in the unlawful distribution of copyrighted material,[44] and the court found that the actions of the website aided and abetted the principal offences of copyright infringement under Swedish law.[45]

---

infringement, is liable for the resulting acts of infringement by third parties." *Id*. at 936–37. After analyzing the conduct of Grokster and Streamcast, the Court found that, insofar as their purpose was to induce their users to infringe copyright, "the unlawful objective is unmistakable." *Id*. at 940.

The notorious file sharing website Napster was found secondarily liable for similar reasons. *See* A&M Records, Inc., 239 F.3d at 1024 (holding that file sharing service which facilitated users' copyright infringement through contributory action was liable for said infringement under 17 U.S.C. § 106).

39. Stockholm Tingsritt [Stockholm District Court] 2009-04-17 B13301-06 (Swed.), *English translation available at* http://www.ifpi.org/content/library/Pirate-Bay-verdict-English-translation.pdf.

40. As with U.S. law, Swedish law requires that, at least for criminal liability, defendants must encourage the "principal offence" (the copyright infringement of individual users). *Id*. at 36.

41. The torrents which The Pirate Bay hosts do not contain files themselves, but rather information that directs a user to the location of different segments of a file. The actual transfer of the file occurs through data transfers over multiple P2P networks. *Id*. at 14. The Pirate Bay website allowed users to upload, store, and download torrent files, it contained a database which allowed users to search for specific torrents, and it contained a tracker which allowed users to contact each other for file sharing. *Id*. at 38.

42. The court found that users had infringed copyright by making the works in question available to the public, in violation of Swedish copyright law. *Id*. at 41–46.

43. The indictment was for "aiding and abetting" an offence under general principles of criminal law, rather than any specific statutory provision relating to liability for copyright infringement. *Id*. at 47. Criminal liability can be established if a defendant aids and abets an offender in either a "physical or psychological sense," and requires that the defendant "must have facilitated the execution of the principal offence." *Id*.

44. *Id*. at 47–48.

45. The court found that:

> [b]y providing a website with advanced search functions and easy uploading and downloading facilities, and by putting individual filesharers in touch with one [an]other through the tracker linked to the site, the operation run via The Pirate Bay has . . . aided and abetted these offences . . . [and] the operation carried on by The Pirate Bay does, objectively, constitute complicity in breach of the Copyright Act.

Stockholm District Court, 2009-04-17 B13301-06 at 48. The Pirate Bay's owners were each sentenced to one year of imprisonment, *id*. at 59, which was later changed to 4–10 months of prison time for each defendant and joint monetary liability of approximately $6.5 million. Jacqui Cheng, *Appeals Court: Pirate Bay Admins Still Guilty, Now With Higher Fines*, WIRED (Nov. 26, 2010, 7:39 PM), http://www.wired.com/threatlevel/2010/11/appeals-court-pirate-bay-admins-still-guilty-now-with-higher-fines/.

The advent of bittorrent, the modern version of P2P software, has made imposing liability for individual infringers difficult. In the U.S., right holders can file "John Doe" lawsuits to compel an ISP to reveal the identity of individual users, but the way that bittorrents operate can make identifying individuals difficult.[46] Despite widespread file-sharing, however, countries have yet to impose any affirmative obligation on ISPs to monitor their websites for infringing activity. A recent EU court decision, *Scarlet Extended SA v. Societe Belge des auteurs, compositeurs et editeurs* ("SABAM"),[47] found that an injunction on an ISP to ensure its users were not file-sharing was in violation of EU law.[48] The High Court of Australia also recently declined to impose such a requirement on the Australian ISP iiNet.[49]

II. ACTA IS AN OUTGROWTH OF THESE EARLIER LEGAL DEVELOPMENTS

Article 27 of ACTA is devoted to "Enforcement In the Digital Environment" and focuses on subjects that, for the most part, either do not appear in or are covered in only a limited fashion in TRIPS and the WIPO Treaty. First, ACTA specifically addresses infringement over digital networks, which neither above treaty discusses.[50] This is an obvious and

46. For a discussion on how bittorrent works, see Colin E. Shanahan, *ACTA Fool or: How Rights Holders Learned to Stop Worrying and Love 512's Subpoena Provisions*, 15 MARQ. INTELL. PROP. L. REV. 465 (2011), *available at* http://scholarship.law.marquette.edu/cgi/viewcontent.cgi?article=1179&context=iplr. Users are not entirely anonymous while downloading files using a torrent, but the software is designed to make a "swarm" of users transfer individual segments of a given file simultaneously, which "allows users to become lost in the swarm, limiting rights holders' ability to identify individual users and prove infringement." *Id.* at 475.

47. Case C-70/10, 2011 E.C.R., *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62010CJ0070:EN:HTML.

48. The court found that requiring the defendant to install a system to filter out infringing content and users would infringe the freedom of the ISP in question "since it would require that ISP to install a complicated, costly, permanent computer system at its own expense," in contravention of EU law requiring the enforcement of IP rights not be "unnecessarily complicated or costly." *Id.* ¶ 48. The court further held that the injunction could infringe the privacy rights of the defendant's customers, because their IP addresses, considered confidential information, would have to be collected and analyzed for the filtering system to work properly. *Id.* ¶¶ 50–51. Finally, the court felt that such a filtering system "could potentially undermine freedom of information since that system might not distinguish adequately between unlawful content and lawful content" and would thus result in potentially filtering out legal content. *Id.* ¶ 52.

49. *See* Roadshow Films Pty Ltd. v. iiNet Ltd. [2012] HCA 16, ¶ 77–80 (Austl.), *available at* http://www.austlii.edu.au/au/cases/cth/FCAFC/2011/23.html (denying an appeal from the Federal Court of Australia which found that iiNet had not "authorized" the file sharing activities of subscribers by not doing anything to stop their acts of copyright infringement).

50. ACTA provides that "each Party's enforcement procedures shall apply to infringement of copyright or related rights over digital networks, which may include the unlawful use of means of widespread distribution for infringing purposes." ACTA, *supra* note 1, art. 27(2).

predictable change of focus, as digital piracy has become so widespread and the legal issues surrounding it remain uncertain. Perhaps the most controversial of ACTA's provisions, and one which appears to take a cue directly from DMCA § 512(h), is the provision allowing parties to compel ISPs to disclose identifying information of alleged infringers.[51] Although this provision requires a "legally sufficient" claim of infringement before disclosure can be compelled, ACTA does not contain any suggestions or minimum standards of what a legally sufficient claim might look like.[52]

While the use of DRM is a controversial issue, the inclusion of provisions on the subject in ACTA is to be expected; both the WIPO Treaty and the DMCA contain provisions regarding its use.[53] Particularly interesting about ACTA's treatment of DRM is that it seems to crib language from DMCA § 512 and adopts the "staple article of commerce" doctrine in determining liability for those circumventing DRM.[54] ACTA thus creates significantly higher international minimum standards for enforcing DRM circumvention than the standards that exist in TRIPS and the WIPO Treaty.

---

51. The provision reads, "[a] Party may provide . . . the authority to order an [ISP] to disclose expeditiously to a right holder information sufficient to identify a subscriber whose account was allegedly used for infringement." *Id*. art. 27(4).

52. ACTA allows a party to compel disclosure of identifying information when a "right holder has filed a legally sufficient claim of trademark or copyright or related rights infringement, and where such information is being sought for the purpose of protecting or enforcing those rights." *Id*. It continues by stating that "[t]hese procedures shall . . . avoid . . . the creation of barriers to legitimate activity . . . and . . . preserve . . . fundamental principles such as freedom of expression, fair process, and privacy." *Id*. While this language certainly appears to be backed by good intentions, it does not contain anything close to the specific limitations on compelled disclosure present in the DMCA.

53. *See* WIPO Treaty, *supra* note 20, arts. 11, 12; *see also* 17 U.S.C. § 1201 (1999).

54. ACTA requires parties to "provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures" used by artists to restrict acts "which are not authorized by the authors." ACTA, *supra* note 1, art. 27(5). ACTA then goes well beyond this general language and creates an obligation for parties to "provide protection at least against" unauthorized circumvention of these measures and "the offering to the public by marketing of a device or product, including computer programs, or a service, as a means of circumventing an effective technological measure." *Id*. art. 27(6)(a).

ACTA also appears to employ the "staple article of commerce" doctrine by requiring members to create legal remedies against

> the manufacture, importation, or distribution of a device or product, including computer programs, or provision of a service that: (i) is primarily designed or produced for the purpose of circumventing an effective technological measure; or (ii) has only a limited commercially significant purpose other than circumventing an effective technological measure.

Id. art. 6(b).

III. HE DOES NOT FIGHT FOR THE USERS:[55] HOW ACTA UNFAIRLY ADVANCES THE INTERESTS OF RIGHTS HOLDERS AT THE EXPENSE OF USERS

As a preliminary matter, it is important to recognize that digital piracy is a serious problem that, despite methodological difficulties in coming up with exact figures,[56] likely costs multiple industries billions of dollars in lost sales every year.[57] Additionally, there is a tremendous disparity between the number of infringers and the number of people held liable for infringement.[58] For these reasons, critics of ACTA do seriously need to consider that the ability of rights holders to profit from their works is substantially threatened by digital piracy. Despite the harm caused by

55. The titular character of the 1982 film *Tron* is a computer program who "fights for the user." *Quotes for Tron*, INTERNET MOVIE DATABASE, http://www.imdb.com/title/tt0084827/quotes (last visited June 29, 2013).

56. For a discussion by the Dutch Government of methodological difficulties in determining the actual economic impact of file sharing and how speculative specific figures by their nature must be, see ANNELIES HUYGEN ET AL., UPS AND DOWNS: ECONOMIC AND CULTURAL EFFECTS OF FILE SHARING ON MUSIC, FILM, AND GAMES 3 (Willemien Kneppelhout et al. trans., 2009), *English translation available at* http://www.ivir.nl/publicaties/vaneijk/Ups_And_Downs_authorised_translation.pdf. In its findings, the study reports that file sharing "provides consumers with access to a broad range of cultural products, which typically raises welfare," despite the fact that "the practice is believed to result in a decline in sales of CDs, DVDs and games." *Id.* The study notes that "[d]etermining the impact of unlicensed downloading on the purchase of paid content is a tricky exercise" because, using music as an example, "one track downloaded does not imply one less track sold" because of the downloaders' possible budget constraints. *Id.* Also, "many people download tracks to get to know new music (*sampling*) and eventually buy the CD if they like it." *Id.*

57. The music, film, and software industries most likely suffer the greatest harm from digital piracy. The Business Action to Stop Counterfeiting and Piracy ("BASCAP") commissioned the London-based organization Frontier Economics to study the economic impact of digital piracy on these industries globally. *See* FRONTIER ECONOMICS, ESTIMATING THE GLOBAL ECONOMIC AND SOCIAL IMPACTS OF COUNTERFEITING AND PIRACY (2011), *available at* http://www.iccwbo.org/Advocacy-Codes-and-Rules/BASCAP/BASCAP-Research/Economic-impact/Global-Impacts-Study/.

The study found that the commercial value of pirated music in 2008 was between $17–40 billion, between $10–16 billion for pirated films in 2005, and between $1.5–19 billion for pirated software, with a notice that the real figures were likely closer to the upper range for each. *Id.* at 30–37. While these figures are for the *value* of pirated works, rather than actual lost sales, they still represent a commercial loss of billions of dollars if even a small percentage of pirating results in lost sales. ACTA's preamble recognizes this, "[*n*]*oting* . . . that the proliferation of . . . services that distribute infringing material . . . causes significant financial losses for right holders and for legitimate businesses." *Id.*

58. While it is extremely difficult to determine with any accuracy how many people engage in digital piracy, a look at the facts of *Grokster* give some indication of the scope of this practice. The Court found that "well over 100 million copies of the software in question are known to have been downloaded, and billions of files are shared . . . each month," making "the probable scope of copyright infringement . . . staggering." Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 923 (2005). On the one hand, this means that a huge number of infringers pirated copyrighted works with impunity. On the other hand, such a tremendous volume of potential defendants would make litigation against all infringers impractical, to say the least.

piracy, however, ACTA's provisions do not strike an effective balance between the interests of rights holders and those of users, both failing to meet one of its stated objectives and failing as a matter of fundamental fairness.[59]

ACTA's language, at least on the surface, gives the impression that parties to the Agreement must consider the rights and interests of users in enacting the Agreement.[60] This language tends to be very broad, however, and when compared with the numerous enforcement and liability provisions which advance the interests of rights holders, appears to offer little more than lip service to ISPs and users. First, ACTA does not require any limitations on liability for ISPs,[61] yet it still allows parties to require ISPs to disclose the identities of alleged infringers.[62] This is a raw deal for ISPs and users, as a party can still compel disclosure from an ISP, but the ISP does not receive any of the "safe harbor" benefits present in the DMCA. For how much of the DMCA ACTA borrows, this is a glaring omission that is potentially prejudicial to internet users.[63]

---

59. ACTA's preamble states that the parties desire "to address the problem of . . . infringement taking place in the digital environment . . . in a manner that balances the rights and interests of the relevant right holders, service providers, and users." ACTA, *supra* note 1, pmbl.

60. *See supra* note 52. The Agreement also contains provisions which call for parties, in implementing procedures pursuant to the Agreement, to "[avoid] the creation of barriers to legitimate activity . . . and . . . [preserve] fundamental principles such as freedom of expression, fair process, and privacy." ACTA, *supra* note 1, art. 27(2).

61. ACTA only touches on ISP liability by stating that a party *may* provide "for limitations on the liability of, or on the remedies available against, online service providers while preserving the legitimate interests of right holder [sic]." ACTA, *supra* note 1, art. 27(2) n.13. Because this language is permissive rather than mandatory, ACTA does not require any party to establish limitations on liability for ISPs. A member of ACTA could thus, while entirely in accordance with the agreement, make ISPs liable for any copyright infringement that takes place on their websites, whether or not the ISP took any steps to encourage the infringement or if it had any knowledge of the infringement.

62. *Id*. art. 27(4).

63. The Computer and Communication Industry Association ("CCIA") has publicly voiced its reservations about some of ACTA's minimum standards for IP protection to the U.S. Trade Representative ("USTR"). It has stated that "ACTA's enforcement-only approach has the effect of promoting U.S. style enforcement provisions without U.S. style exceptions to those provisions," and that omissions of "fair use or any of the other exceptions and limitations in U.S. law upon which exporters depend constitutes a missed opportunity to promote opportunities for U.S. Industry." Matthew Schruers, *Comments of the Computer and Communications Industry Association on the Anti-Counterfeiting Trade Agreement*, at 2–3 (Feb. 15, 2011), *available at* http://infojustice.org/wp-content/uploads/2011/02/CCIA-Comments-to-USTR.pdf. The CCIA also tied such exceptions to economic growth, citing research indicating that in the U.S. in 2010, industries relying upon these exceptions generated $281 billion in goods and services. *Id*. at 3 (citing THOMAS ROGERS & ANDREW SZAMOSSZEGI, FAIR USE IN THE U.S. ECONOMY: THE ECONOMIC CONTRIBUTION OF INDUSTRIES RELYING UPON FAIR USE 6 (2010), *available at* http://www.wired.com/images_blogs/threatlevel/2010/04/fairuseeconomy.pdf). It encourages the USTR to "export . . . a fair use concept overseas," and argues that agreements like ACTA constitute a failure to do so. Schruers, *supra*, at 7. The CCIA feels that an agreement like ACTA which "facilitates strong enforcement without encouraging fair use and

ACTA also contains procedural deficiencies in its allowance for provisional measures.[64] ACTA borrows much of its provisional measures language from TRIPS, allowing for provisional measures to be taken *inaudita altera parte*.[65] A significant difference between TRIPS and ACTA, however, is that ACTA drops the TRIPS requirement for notice to the affected party; it only requires that an applicant provide evidence and a security.[66] Further, ACTA requires that members provide for injunctive relief in civil suits, but it does not indicate under what circumstances such relief should be available.[67] This is yet another conspicuous omission, as injunctive relief is an extraordinary remedy and should not be granted lightly. U.S. law, for example, has specific requirements for when an injunction can be issued in a copyright infringement claim.[68]

ACTA does not contain any specific section or provision on limitations or exceptions like those present in TRIPS and the WIPO Treaty. The language promoting "fundamental principles such as freedom of expression, fair process, and privacy" are a nice thought, but are less protective of users than even the anemic limitations present in ACTA's two predecessor treaties.[69] The inclusion of explicit defenses may not be

---

other exceptions will have the practical effect of promoting a copyright framework that is inconsistent with U.S. law and harmful to U.S. businesses." *Id*.

64. *See* ACTA, *supra* note 1, art. 12.

65. *Id*. art. 12(2).

66. ACTA only mandates that judicial authorities require an applicant to "provide any reasonably available evidence in order to satisfy themselves . . . that the applicant's right is being infringed or that such infringement is imminent, and to order the applicant to provide a security . . . ." *Id*. art. 12(4). Parties have discretion in determining what may constitute a security, but ACTA specifies that it may be "in the form of a bond conditioned to hold the defendant harmless from any loss or damage resulting from" inspection or detention of any goods in the event of non-infringement. *Id.* art. 18. There is at least one redeeming feature in this section, however, as it provides that "where it is subsequently found that there has been no infringement . . . the judicial authorities shall have the authority to order the applicant . . . to provide the defendant appropriate compensation for any injury caused by these measures." *Id*. art. 12(5).

67. *Id.* art. 8(1).

68. Injunctive relief is not automatically awarded upon a finding of copyright infringement. To be awarded injunctive relief, the plaintiff in any type of intellectual property infringement claim must satisfy a four-element test. The plaintiff must show:

> (1) that it has suffered an *irreparable* injury; (2) that remedies available at law, such as monetary damages, are inadequate to compensate for that injury; (3) that, considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction.

eBay Inc. v. MercExchange, L.L.C., 547 U.S. 388, 391 (2006) (emphasis added); *see also* WILLIAM F. PATRY, 6 PATRY ON COPYRIGHT § 22:74 (2011).

69. Article 10 of the WIPO Treaty explicitly allows parties to create exceptions, and by implication, TRIPS allows them. ACTA, by contrast, only allows "a party [to] adopt or maintain appropriate limitations or exceptions to measures implementing the provisions" related to DRM circumvention. ACTA, *supra* note 1, art. 27(8). Not only are these limitations vague, their exclusion in

necessary for countries such as the U.S. that have copyright law with robust and well-established bodies of case law that include defenses such as fair use,[70] but not all parties to ACTA have such defenses. For example, a recent court decision in Belgium, *Copiepresse v. Google*, found the search engine Google liable for copyright infringement because it allowed access to "cached" versions of copyrighted newspaper articles. There is little question that this practice would be allowed under U.S. law,[71] indicating that even European countries can be much more restrictive than the U.S. in their defenses to copyright infringement.[72]

---

other provisions of the Agreement may suggest that they do not apply elsewhere. Kaminski, *supra* note 8, at 395.

Provisions on fair use and other common defenses to copyright infringement are entirely absent in ACTA. Likewise, neither TRIPS nor the WIPO Treaty define such exceptions, but it is disconcerting that ACTA, in establishing much higher international standards for infringement and enforcement, does not balance such new standards with new limitations.

70. For examples of fair use jurisprudence in the digital environment, see Kelly v. Arriba Soft Corp., 336 F.3d 811 (9th Cir. 2003) (holding that a search engine which stores and displays low-resolution "thumbnails" of copyrighted images engaged in a fair use of those images because they were used for only an incidentally commercial purpose and, because the thumbnail images served a different purpose from original images, they were transformative); Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146 (9th Cir. 2007) (holding that the transformative aspects of thumbnail images in a search database outweigh the speculative harm caused by potential customers downloading such thumbnails to their phones instead of purchasing the images from the artist); Field v. Google Inc., 412 F.Supp.2d 1106, 1123 (D. Nev. 2006) (affirming *Kelly* and extending the Ninth Circuit's decision to cached copies of copyrighted works, finding that cached web pages are present for a transformative, rather than superseding, purpose and are therefore a fair use).

71. Cases such as *Kelly v. Arriba Soft* and *Field v. Google* would likely dictate a finding of non-infringement in these instances, especially since the news stories were not available in their entirety through cached pages.

72. The Belgian court of appeals for Brussels found that Google's practice of "caching" (storing snapshots of web pages on a searchable database that are accessible even after the content is no longer reachable through its search engine) constituted copyright infringement. La Cours d'appel (CA) [Court of Appeal] de Bruxelles, May 5, 2011 (Belg.), *English translation available at* http://static.arstechnica.com/CopiepresserulingappealGoogle_5May2011.pdf.

The court found that Google's caching of newspaper articles did not fall within the caching exception of EU Directive 2001/29's preamble 33, because it did not show that caching was "an intrinsic and essential part of a technological process . . . enabling efficient transmission in a network between third parties . . . by an intermediary . . . ." *Id.* ¶ 25 (internal quotation marks omitted). The court was also not convinced that Google's caching of the articles was sufficiently "transient" to fall within the directive's exceptions, holding that "[a]n act of reproduction can be qualified as 'transient' . . . only if its duration is limited to what is necessary for the proper completion of the technological process in question," and that the reproduction will be automatically deleted when the process has been completed. Because Google's cached version of a given article remains available free of charge for as long as the website hosting the article makes it available, the court held that Google could not enjoy this exception, either. *Id.* ¶ 26.

The Belgian court further held that the Google News service's practice of copying short excerpts from news articles also constituted copyright infringement. It felt that the purpose of this practice was to, in effect, supplant the original news story by "allow[ing] readers to find out the essential information the publisher and journalist wanted to convey," because readers could understand the main

It may seem counter-intuitive to argue that an increase in digital piracy should necessitate international enforcement standards to be friendlier to users and ISPs, but legislation that has been and currently is created in response to digital piracy illustrates why an international IP scheme should show major concern for the rights of users and ISPs. In early 2012, The U.S. House of Representatives was scheduled to vote[73] on the intensely unpopular Stop Online Piracy Act ("SOPA"),[74] which was strongly opposed by a large number of persons and companies within the technology industry, as well as consumers' rights groups.[75] While ostensibly directed at foreign "rogue" websites that host infringing content but either do not comply with DMCA takedown requests or are outside of U.S. jurisdiction, the bill contained provisions that would have affected legitimate American businesses as well. The payment processors and/or advertisers for an allegedly infringing website would have only five days in which to comply with a termination notice, and the owners of the website would have an equally small window in which to file a response explaining why they were not infringing the rights of the complainant to avoid being cut off from funds or advertising.[76] This provision, as SOPA's detractors contended, would allow a rights holder to effectively terminate the funding for websites and shut them down without any finding of copyright infringement, even if the party filing the complaint does not have any rights to the work in question. Review of the termination notice can occur after action has been taken, but in many cases the damage will have already been done.[77] Other criticisms include allegations that SOPA

---

events of a given story within Google's short excerpt and would thus not need to read the entire article unless they wanted additional details. *Id*. ¶ 28.

73. House Majority Leader Eric Cantor suspended a vote on the Stop Online Piracy Act ("SOPA"), claiming that he would "not bring the bill to the floor unless there's real consensus on the bill." Mike Masnick, *SOPA Delayed; Cantor Promises It Won't Be Brought To The Floor Until 'Issues Are Addressed,'* TECHDIRT (Jan. 13, 2012, 11:57 PM), http://www.techdirt.com/articles/20120113/23560217407/sopa-delayed-cantor-promises-it-wont-be-brought-to-floor-until-issues-are-addressed.shtml.

74. H.R. 3261, 112th Cong. (2011).

75. Some of SOPA's more notable opponents include American Express, AOL, eBay, Google, YouTube, Reddit, Tumblr, Twitter, Yahoo!, Daily Kos, the ACLU, and several video game companies. *See List of Those Expressing Concerns with SOPA & PIPA*, CTR. FOR DEMOCRACY AND TECH. (Jan. 15, 2012), http://www.cdt.org/report/list-organizations-and-individuals-opposing-sopa (last updated Jan. 25, 2012).

76. H.R. 3261, 112th Cong. §§ 103(b)(1)–(2), (5) (2011).

77. *See* Corynne McSherry, *SOPA: Hollywood Finally Gets a Chance to Break the Internet*, ELECTRONIC FRONTIER FOUNDATION (Oct. 28, 2011), https://www.eff.org/deeplinks/2011/10/sopa-hollywood-finally-gets-chance-break-internet. McSherry criticizes the short 5-day window which payment processors for allegedly infringing websites have to comply with infringement notices. *Id.* She argues that it is extremely difficult for allegedly infringing sites to prepare a sufficiently thorough response to a notice during this time period, and that payment processors have no obligation to abide

would violate the First Amendment[78] and human rights, as well as endanger whistleblowers.[79] Though SOPA may not be permissible under current U.S. law, it appears to be fully compliant with ACTA.

The Spanish government in 2012 enacted legislation that appears to be similar to SOPA. The so-called Sinde Law provides for measures that "will give the authorities the power to swiftly close file-sharing sites or have them blocked at the ISP level" within ten days of a complaint by right holders.[80] In Italy, legislation is currently under consideration that might require ISPs to filter services that infringe copyright and could

---

by them even if one is made. Essentially, this would incentivize right holders to send out a flurry of "bogus complaints" in the hope of effectively shutting down current or potential competitors. *Id.*

SOPA also includes a provision that would make the streaming of ten or more copyrighted works in a 6-month period online "for purposes of commercial advantage or private financial gain" a felony. H.R. 3261, § 201. Because the "commercial advantage or private financial gain" language is open to interpretation, it could arguably include websites that possess any type of revenue stream or advertising income, even if the streaming itself is not intended for any type of financial gain.

78. *See* Laurence H. Tribe, *The "Stop Online Piracy Act" (SOPA) Violates the First Amendment* (Dec. 6, 2011), *available at* http://www.scribd.com/doc/75153093/Tribe-Legis-Memo-on-SOPA-12-6-11-1. Harvard professor Tribe argues that § 103(a) of SOPA, which covers notice and termination procedures for allegedly infringing websites violates the prior restraint doctrine because:

> it delegates to a private party the power to suppress speech without prior notice and a judicial hearing. This provision of the bill would give complaining parties the power to stop online advertisers and credit card processors from doing business with a website, merely by filing a unilateral notice accusing the site of being "dedicated to theft of U.S. property"—even if no court has actually found any infringement. The immunity provisions in the bill create an overwhelming incentive for advertisers and payment processors to comply with such a request immediately upon receipt.

Id. at 1.

Tribe also argues that because of SOPA's ambiguities in defining which websites fall under the definition of "dedicated to theft of U.S. Property," many websites will in effect have to monitor their websites for infringing activity, even if no complaint of such activity is made. *Id.* at 2. This is an intrusive obligation not present in the DMCA and would likely lead to a chilling effect by which websites would not engage in constitutionally protected speech "for fear that they will be accused of a SOPA violation and suffer a cutoff of revenue from online advertising or credit card payments for transactions," thereby chilling innovation of internet companies. *Id.* at 2–3.

79. *See* Trevor Timm, *Proposed Copyright Bill Threatens Whistleblowing and Human Rights*, ELECTRONIC FRONTIER FOUND. (Nov. 2, 2011), https://www.eff.org/deeplinks/2011/11/proposed-copyright-bill-threatens-whistleblowing-and-human-rights (arguing that provisions enabling private individuals to give takedown notices "could target websites behind important Internet projects such as Tor, the anonymity network that has been vital for protecting activists from government surveillance in Tunisia and Egypt."). *Id.* Because the website can be used to mask one's IP address while downloading content, "[c]orporations concerned about users illegally downloading music could use SOPA to force Visa and Mastercard to cut off donations to Torproject.org—despite Tor's aim to facilitate human rights activism, not piracy." *Id.* These criticisms also concern SOPA's applicability to sites such as Wikileaks, which encourage whistleblowing.

80. *See Website Blocking Law Implemented By New Spanish Government*, TORRENT FREAK (Jan. 2, 2012), http://torrentfreak.com/website-blocking-law-implemented-by-new-spanish-government-120102/.

blacklist individual users who are only accused of infringement.[81] France and the U.K., among other parties to ACTA, are either considering or have already enacted "three strikes" laws that allow authorities to blacklist users or ISPs for repeated instances of copyright infringement.[82]

IV. WHAT A BETTER, FAIRER IP TREATY MIGHT LOOK LIKE

With ACTA's future steadily becoming less certain, future IP treaties concerned with copyright infringement would do well to look at the Agreement's shortcomings and address them accordingly. The digital copyright infringement provisions of ACTA address a serious problem, but the Agreement's most serious deficiency is that it does not attempt to provide limitations on the new authority it grants to parties. Enumerating limitations and exceptions, both mandatory and permissive, could make ACTA much more balanced.[83] In the case of compelling ISP disclosure of the identity of alleged infringers, the Agreement could also simply adopt the "safe harbor" provisions of the DMCA,[84] which would make the document considerably less hostile to ISPs. ACTA's purely permissive language about limiting liability for ISPs is also woefully inadequate[85] and allows for overly restrictive legislation to be enacted in countries with less

81. *See* Loek Essers, *Italy Prepares 'One Strike' Anti-piracy Law*, PC WORLD (Sept. 22, 2011, 4:10 PM), http://www.pcworld.com/businesscenter/article/240413/italy_prepares_one_strike_antipiracy_law.html; *see also* Timothy B. Lee, *UN Report: "Three Strikes" Internet Laws Violate Human Rights*, ARS TECHNICA (June 3, 2011, 3:20 PM), http://arstechnica.com/tech-policy/news/2011/06/un-free-speech-watchdog-blasts-three-strikes-rules.ars.

82. *See* Alberto J. Cerda Silva, *Enforcing Intellectual Property Rights By Diminishing Privacy: How the Anti-Counterfeiting Trade Agreement Jeopardizes the Right to Privacy*, 26 AM. U. INT'L L. REV. 601 (2011). Silva identifies the concept of "three-strikes" internet laws as "a domestic legal mechanism allowing the disconnection of a supposed infringing Internet user . . . after the user has received warnings about, and failed to cease copyright infringement occurring via his Internet account." *Id.* at 630. He further discusses how such policies are fully in line with ACTA's provisions, and how early drafts of the Agreement actually encouraged the adoption of three-strikes policies, but have since backed off such advocacy due to unpopularity and disagreement during negotiations. *Id.* at 633–34.

83. For an example of specific limiting language in a multi-national document, see Council Directive 2001/29, 2001 O.J. (L 167) (EC). This EU directive provides for numerous exemptions to copyright holders' rights, such as reproduction for educational purposes, parody, criticism, and various non-commercial uses. *Id.* art. 5. While these limitations are almost entirely permissive, rather than mandatory, and their allowance is confined to the "do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the rightholder" language in TRIPS and the WIPO Treaty, they at least recognize the balancing of interests of rights holders and users as a priority. *Id.* art. 5(5); *see also* TRIPS, *supra* note 2, art. 13; WIPO Treaty, *supra* note 20, art. 10.

84. 17 U.S.C. § 512(a)–(d) (1999).

85. ACTA, *supra* note 1, art. 27 n.13.

well-defined bodies of law regarding digital copyright infringement or less robust defenses for infringement.[86]

A simple adjustment to ACTA that would help to balance out some of the Agreement's weaknesses could be the elimination of provisions that require parties to adopt principles of secondary liability for copyright infringement.[87] Not all parties to ACTA have well-established principles of secondary liability, if such principles exist at all.[88] Imposing this legal concept onto the courts and legislatures of countries without a pre-existing framework for imposing and limiting such liability could lead to unintended consequences for websites with substantial international operations.[89] There is a problem with excluding the requirement of secondary liability, though; because file sharers are so difficult to identify and track down, rights holders would likely not have a particularly effective means of preventing the infringement of their works without the ability to bring suit against ISPs. To strike a balance between protecting rights holders' interests and those of ISPs, ACTA could explicitly define *maximum* standards for imposing secondary liability which its parties could not exceed. Considerable deliberation would be necessary in ensuring these standards accommodate the needs of each member nation, but the DMCA again provides a good starting point.

Perhaps it is too optimistic to hope for a new limitation on an old concept, but ACTA is a missed opportunity to address the controversy surrounding the use of DRM and how it might contribute to, rather than prevent, digital infringement. A common reason for file sharing given by opponents of the practice is the desire to get something for nothing, essentially to "steal" the copyrighted content.[90] If this content is protected

86. Belgian law, for example, does not have a fair use defense that is comparable to U.S. law, and EU law does not fill this gap. *See, e.g.*, La Cours d'appel (CA) [Court of Appeal] de Bruxelles, May 5, 2011 (Belg.). Spain and Italy, among other countries, are also in the midst of creating and enacting legislation that imposes excessive liability on ISPs for the copyright infringement of their users. *See Website Blocking Law Implemented By New Spanish Government*, *supra* note 80; *see also* Essers, *supra* note 81. The Dutch parliament, however, has recently introduced a bill that would explicitly allow users to create remixes and "mashups" of copyrighted works. Robert Chesal, *Loosen Up Copyright Law, Says Dutch Government*, RADIO NETH. WORLDWIDE (Feb. 13, 2012, 10:03 AM), http://www.rnw.nl/english/article/loosen-copyright-law-says-dutch-government.

87. ACTA, *supra* note 1, art. 27(6).

88. *See* Schruers, *supra* note 63, at 9.

89. In his letter to the USTR, Schruers points out that because secondary liability is absent in both multilateral IP treaties and the domestic law of many countries, "including secondary liability in ACTA would represent a major change in the framework of international IP law, and would go far beyond the enforcement focus of ACTA." *Id.*

90. For a discussion of the ideological camps in the debate surrounding DRM, see generally Declan McCullagh & Milana Homsi, *Leave DRM Alone: A Survey of Legislative Proposals Relating to*

by restrictive DRM, however, then file sharers may copy the content simply because a "pirated" copy of it is superior to the original, as it lacks any restrictions.[91] Particularly for movies and music, restrictions on the ability to reinstall or make backup copies of content for personal use[92] may deter customers who are entirely capable of and willing to pay for content from acquiring it through official channels. This is not to argue that ACTA should condemn the entire practice of implementing DRM, but a modern treaty concerned with digital copyright infringement should be willing to acknowledge that DRM potentially creates a power imbalance between rights holders and users and should provide a more nuanced treatment of it than what is present in the DMCA and ACTA's predecessor treaties.

A final minor adjustment to ACTA's language that would make it more palatable would be the removal of statutory damages as a remedy for copyright infringement.[93] It may be tempting to include the availability of statutory damages as a strong deterrent to digital piracy, as the U.S. has done, but such a framework can lead to damage awards that are incommensurate with the offense committed. Since copyright infringement is a civil action between private individuals, the severity of punitive or deterrent damages should be reined in. In cases of websites that

---

Digital Rights Management Technology and Their Problems, 2005 MICH. ST. L. REV. 317 (2005), *available at* http://msulawreview.org/PDFS/2005/1/McCullagh-Homsi.pdf.

91. For a discussion of this scenario and the merits of various proposed DRM schemes, see generally Joshua J. Dubbelde, *A Potentially Fatal Cure: Does Digital Rights Management Ensure Balanced Protection of Property Rights?*, 2010 U. ILL. J.L. TECH. & POL'Y 409 (2010), *available at* http://www.jltp.uiuc.edu/archives/dubbelde.pdf.

92. For example, prior to 2009, the Apple software program iTunes implemented DRM that allowed only Apple devices to play music that had been purchased through iTunes. Ruth Suehle, *The DRM Graveyard: A Brief History of Digital Rights Management in Music*, OPENSOURCE (Nov. 3, 2011), http://opensource.com/life/11/11/drm-graveyard-brief-history-digital-rights-management-music. Overly restrictive DRM measures may also contribute to users pirating video games. One of the least popular DRM measures for computer games is a limitation on the number of times players can install a given copy of a game; while this may prevent illegal copying, it also means that players who upgrade their computers or format their hard drives may be unable to play the game. *See* Andy Greenberg & Mary Jane Irwin, *Spore's Piracy Problem*, FORBES (Sept. 12, 2008, 10:00 AM), *available at* http://www.forbes.com/2008/09/12/spore-drm-piracy-tech-security-cx_ag_mji_0912spore.html (discussing the popular 2008 computer game "Spore," and how its DRM which restricts players to three installations of the game before having to purchase another copy may have been a reason that an unusually large number of people pirated the game).

93. The agreement requires parties to "establish or maintain a system that provides for . . . pre-established damages." ACTA, *supra* note 1, art. 9(3)(a). While this is not an absolute requirement, as other forms of damages can be chosen in lieu of pre-established damages, ACTA still provides a framework that allows extremely large mandatory fines even in individualized cases of copyright infringement for no commercial purpose.

are charged with repeat offenses, the damage awards can become comedically large,[94] as if something out of an Austin Powers movie.[95]

ACTA could also look to legislation that emphasizes users' rights for some ideas on how to balance its provisions. Its drafters could take some cues from Brazil's proposed Marco Civil da Internet law,[96] which treats access to, and use of, the internet as a civil right. While the most recent draft of the legislation has stripped many of its earlier protections,[97] the original version severely limited ISP liability,[98] the ability to cut off users from the internet,[99] and the ability to subpoena ISPs for user information.[100] The specific provisions of this proposed law may not be wise for IP maximalist countries to adopt in the face of rampant digital piracy, but Brazil's approach seems to offer a much preferable alternative to the draconian internet blacklisting laws under consideration in the U.S. and EU.

These recommendations would not just benefit ISPs and users either; given the reactions to ACTA worldwide and SOPA in the U.S., it has

---

94. *See* Tom Corelis, *RIAA Drops $1.65T AllofMP3 Lawsuit, Claims Victory*, DAILY TECH (May 28, 2008, 4:31 AM), http://www.dailytech.com/RIAA+Drops+165T+AllOfMP3+Lawsuit+Claims+Victory/article11882.htm (discussing the later-dropped RIAA lawsuit against Russian file sharing site AllofMP3, seeking the maximum U.S. statutory damage amount of $150,000 per copyright infringement, thus resulting in total requested damages of $1.65 trillion).

95. In *Austin Powers: The Spy Who Shagged Me*, the villain, Dr. Evil, threatens to destroy several major U.S. cities unless he is paid 100 billion dollars by the federal government. As this scene is set in 1969, the U.S. president replies that asking for this sum is the same as asking for "a kajillion bajillion dollars." *Quotes for Dr. Evil*, INTERNET MOVIE DATABASE, http://www.imdb.com/character/ch0026630/quotes (last visited Jan. 11, 2013).

96. Decreto No. 00086, de 25 de April de 2011, DIARIO OFICIAL DA UNIAO [D.O.U.] de 4.25.2011 (Braz.), *English translation available at* http://www.a2kbrasil.org.br/wordpress/wp-content/uploads/2011/09/Marco-Civil-Ingle%CC%82s-pm.pdf.

97. *See* Carolina Rossini, *New Version of Marco Civil Threatens Freedom of Expression in Brazil*, ELECTRONIC FRONTIER FOUND. (Nov. 9, 2012), https://www.eff.org/deeplinks/2012/11/brazilian-internet-bill-threatens-freedom-expression.

98. The legislation states that "[i]nternet connection providers shall not be responsible for damage arising from content generated by third parties." Decreto No. 00086, art. 14. The only exception to this is "if, after receiving a specific judicial order, they do not take action to, in the context of their services and under the established time frame, make unavailable the infringing content." *Id*. art. 15. This is in marked contrast to ACTA's language which permits rights holders to send infringement notices to ISPs or their payment providers/advertisers which, absent a response, can compel action without a court order. ACTA, *supra* note 1, arts. 8, 12; *see also supra* note 67.

99. The legislation guarantees these rights to users: "the non-violation and secrecy of communications on the Internet, except under judicial order . . . for criminal investigations or the gathering of evidence for criminal procedures," and "the non suspension of Internet connections, except for debts directly related to their use." Decreto No. 00086, art. 7(I)–(II).

100. A request for disclosure of identifying information of an alleged user must contain "evidence of the occurrence of an illegal act; . . . justification for the utility of accessing the requested logs, for the purposes of investigation or the gathering of evidence; [and] . . . the period that the logs refer to." *Id*. art. 17.

become apparent that restrictions on online conduct are increasingly unpopular. Finland, for example, has made 1Mbps internet access a legal right,[101] and one of the stated goals of Sweden's Pirate Party is to make all non-commercial copying free.[102]

CONCLUSION

On its face, ACTA could be seen as an international agreement with the noble intention of combating a serious economic problem in today's society, as well as a necessary adaptation of international law on a quickly mutating body of law. To those unfamiliar with how the internet and file sharing work, its provision might look proportionate, necessary, and effective. In reality, however, ACTA is a rocket-powered sledgehammer where a surgical laser is required, at least regarding its provisions on copyright infringement in the digital environment.

While increasingly strict digital copyright enforcement is inevitable in the face of a growing and changing tech industry, ACTA's harsh measures show a disconnect with reality. The content of article 27 of the agreement, combined with its general provisions on enforcement and remedial measures, displays either a willingness to throw the rights of users and ISPs under the proverbial bus to benefit rights holders, or a lack of awareness as to precisely what the implications and possible consequences of such provisions are.

Even though the Agreement has softened somewhat since its initial drafts (which received especially scathing criticism), it is still a failure at balancing the rights of users and ISPs with those of rights holders. Considering how many of the concepts and how much language from ACTA appear to have been taken directly from U.S. law, particularly the DMCA, it is startling to see such a pronounced lack of balance within the agreement when U.S. law provides so many templates for defenses and exceptions to copyright infringement and liability. It is still possible for a country to adopt the agreement in a reasonable, balanced fashion, yet ACTA also permits strict legislation such as SOPA and three-strikes laws. It is precisely because of ACTA's failure to provide explicit limitations on

101. *See Finland Makes Broadband a 'Legal Right,'* BBC NEWS (July 1, 2010), http://www.bbc.co.uk/news/10461048. The Finnish government has further plans to increase this legally guaranteed speed to 100Mbps by 2015. *Id.*

102. *See Pirate Party Principles*, PIRATPARTIET, http://www.piratpartiet.se/politik/piratpartiets-principer/ (last visited June 29, 2013). In 2009, the Pirate Party won a seat in the EU parliament. Ernesto, *How Pirates Shook European Politics*, TORRENTFREAK (June 8, 2009), http://torrentfreak.com/how-pirates-shook-european-politics-090608/.

liability, defenses to copyright infringement, and robust procedural safeguards for rights holders to bring claims of infringement that this type of legislation would be possible even if ACTA were ratified.

As a final testament to ACTA's misguided approach to imposing enforcement standards, it could very well lead to significant financial harm to countries which decide to adopt it in restrictive fashions. Strong DRM measures may actually contribute to piracy because users do not want to deal with the multiple restrictions placed upon legitimate copies of software. Further, the types of extended secondary liability that parties are permitted to place on ISPs under ACTA could very well stifle innovation, preventing potentially job-creating businesses from ever getting off the ground or expanding for fear that some of their users might cause them to become the target of a rights holder's complaint. When compared to the speculative figures for harm caused by digital piracy and file sharing, the economic benefits of ACTA and its enacting legislation become uncertain, at best.

Alex Shepard[*]

---

* J.D. (2013), Washington University School of Law; B.A. (2009), University of Tennessee at Chattanooga. Alex Shepard thanks the many Global Studies Law Review board members who were willing to fix his typographical and citation errors, which were legion. He also thanks his friends, classmates, and members of the Washington University School of Law faculty who offered him guidance on writing this note.