POSITIVE PROPOSALS FOR TREATMENT OF ONLINE INTERMEDIARIES

MARGOT KAMINSKI*

* Executive Director of the Information Society Project at Yale Law School and Research Scholar and Lecturer in Law.

I. INTRODUCTION

In the past several years of free trade agreement negotiations, a number of proposals for establishing an international standard of liability for copyright infringement by online intermediaries have emerged.[1] These proposals consistently lack consideration of their implications for Internet users. Building off a public stakeholder presentation given by the author at the ninth round of negotiations of the Trans-Pacific Partnership ("TPP") Agreement, held in Lima, Peru, this paper aims to identify both general principles and specific user-protecting provisions that should be considered when discussing proposals for intermediary liability.

II. THE PROBLEMS RAISED BY INTERMEDIARY LIABILITY

This section provides a brief overview of the problems inherent in establishing liability for online intermediaries.[2] Online intermediaries host a vast variety of content provided by Internet users. In fact, all online communication passes through an intermediary of some sort, whether it is an Internet Service Provider ("ISP"), such as Comcast, or a platform, such as Google or Facebook. Intermediary behavior directly affects users' freedom of expression, privacy, and ability to innovate. An intermediary may also choose to monitor users' behavior, take down user-created content, or prevent the construction of new technology on the platform it provides. An ISP may undertake

1. Discussions of intermediary liability have arisen in negotiations for the Anti-Counterfeiting Trade Agreement (ACTA) and in the ongoing Trans-Pacific Partnership Agreement (TPP) negotiation rounds. *See* Margot E. Kaminski, *An Overview and the Evolution of the Anti-Counterfeiting Trade Agreement*, 21 ALB. L.J. SCI. & TECH. 385 (2011) [hereinafter Kaminski, *Anti-Counterfeiting*]; Margot Kaminski, *Plurilateral Agreements Lack Protections for Users, Intermediaries*, INTELL. PROP. WATCH (Oct. 27, 2011, 11:47 PM), http://www.ip-watch.org/2011/10/27/plurilateral-trade-agreements-lack-protections-for-users-intermediaries/ [hereinafter Kaminski, *Plurilateral Agreements*].

2. Thanks to Matthew Zimmerman at the Electronic Frontier Foundation for his helpful slide presentation. Mathew Zimmerman, *Freedom of Expression, Indirect Censorship & Liability for Internet Intermediaries*, ELEC. FRONTIER FOUND. (Feb. 15, 2011), *available at* https://www.eff.org/issues/tpp (follow "EFF Presentation on Freedom of Expression, Indirect Censorship & Liability for Internet Intermediaries" hyperlink).

these actions independently or at the request of a government.

When a government establishes legal liability for intermediaries, it affects intermediaries' behaviors and, thus, affects Internet users. For example, making an online platform liable for its users' defamation will likely cause the intermediary to take down a large number of user comments out of caution.[3] Similarly, making an email-hosting service liable for the content of a user's email would cause that intermediary to monitor the content of the user's inbox to make sure nothing potentially damaging is being sent or received.[4] Finally, making a smartphone provider liable for legal problems with third-party applications built on its operating system would make that intermediary more likely to reject new technologies.[5]

None of these actions stems from malice on the part of the intermediary. They come from a company's reasonable caution, in the light of potential damages or criminal punishment. In other words, Yahoo!'s lawyers will look at the intermediary liability system that a government sets up; calculate the risk Yahoo! faces with its current policies, taking intermediary liability laws into account; and give advice to their client that is sound and cautious. But such measures greatly influence users' ability to use Yahoo! to communicate.

Consequently, governments need to be particularly careful when establishing systems of intermediary liability. When a company faces the prospect of intermediary liability, it is unlikely that users' interests will be its primary focus.[6] The company may consider

3. *See Comments of CDT to the DG Internal Market and Services, Regarding Notice-and-Action Procedures by Internet Intermediaries*, CTR. FOR DEMOCRACY & TECH. 1 (2012), *available at* https://www.cdt.org/files/pdfs/CDT-Comments-Notice-and-Action.pdf (noting that "[w]hen intermediaries are liable for the content created by others, they will strive to reduce their liability risk, which can lead to over-blocking of legitimate content").

4. *See id.* at 5 (explaining that monitoring obligations would undermine the ability of intermediaries to offer robust online services that facilitate communication without jeopardizing user privacy).

5. *See, e.g.*, Kendra Albert, Nick Fazzio, & Jonathan Zittrain, *Taking More Than Candy from a Baby*, THE FUTURE OF THE INTERNET AND HOW TO STOP IT BLOG (June 13, 2012), http://futureoftheinternet.org/taking-more-than-candy (noting that Apple pulled an app from its app store for fear of being drawn into litigation and, in particular, being found liable for secondary patent infringement).

6. *See, e.g.*, *id.* (describing how Apple removed an app from its app store that

potential market backlash to its reaction to intermediary liability laws. However, if the liability exposure is great enough, long-term user preferences will often take the backseat to avoiding an immediate lawsuit.

In summary, intermediary liability encourages intermediaries to prevent content from being posted in the first place, take down legitimate content, choke innovative new technology built on their platforms, or perform surveillance on users.[7] These measures generally undercut user privacy and freedom of expression.

There is also a public choice problem.[8] The highest stakeholders in intermediary liability—the potential plaintiff and the potential defendant—have greater incentive to craft liability laws than Internet users, whose interests are diffuse and who face higher organizational costs.[9] Governments must, therefore, be especially attentive to including protections for the general public when considering intermediary liability legislation.

Recognizing that intermediaries' interests are not perfectly aligned with user interests, this paper aims to identify the kinds of user protections that governments should be sure to include in intermediary liability regimes.

III. WHAT INTERMEDIARIES CAN BE TOLD TO DO—OR NOT TO DO

Governments have a number of choices for how to treat online intermediaries. They can go after the intermediary directly, by making it criminally liable for user behavior.[10] They can make the

facilitated an autistic child's ability to communicate to avoid secondary liability for patent infringement).

7. *See generally* CHILLING EFFECTS, http://www.chillingeffects.org/ (last visited July 17, 2012) (cataloguing cease-and-desist notices to Internet users and documenting the chilling effects of intellectual property laws on First Amendment rights online).

8. *See* WILLIAM M. LANDES & RICHARD A. POSNER, THE POLITICAL ECONOMY OF INTELLECTUAL PROPERTY LAW 13–16 (2004) (explaining the asymmetry between private benefits that would arise from strong intellectual property rights versus denying intellectual property rights).

9. *See id.* at 8–11.

10. Rachel Donadio, *Larger Threat Is Seen in Google Case*, N.Y. TIMES, Feb. 25, 2010, http://www.nytimes.com/2010/02/25/technology/companies/

intermediary civilly liable to other private parties for monetary damages.[11] They can directly require the intermediary to monitor user behavior or indirectly create incentives to monitor users through the implementation of a liability regime. They can encourage an intermediary to take down material as part of a notice-and-takedown regime,[12] or they can require an intermediary to cut off a user's Internet access.[13]

The United States operates under a system of notice-and-takedown. The United States limits intermediary liability, provided that the intermediary takes down infringing material when it has been notified of it and then replaces that material in response to claims that it is not, in fact, infringing.[14] The Digital Millennium Copyright Act ("DMCA"), the statutory authority for intermediary liability in the United States, falls under civil law, not criminal law, and depends upon the presumption that intermediaries are liable for user behavior in the first place.[15] It is also worth noting, as I discuss briefly in the next section, that the DMCA addresses copyright only; in the United States, intermediaries are not liable for user defamation or other actions. The DMCA recognizes a variety of intermediaries, including both platforms and pipes, and treats them differently based on how much control the intermediary can (and does) exercise over the content passing through it.[16] For example, neutral, noninterfering pipes (such as the fiber networks that form the backbone of the

25google.html?pagewanted=all (discussing an Italian court holding three Google executives criminally liable for content posted on its system); *see also* Sentenza n. 1972/2010, Tribunale Ordinario di Milano in Composizione Monocratica, Sezione 4 Penale [Judgment no. 1972/2010, Ordinary Court of Milan with a single judge, Section 4 Criminal] (Apr. 12, 2010), *available at* http://speciali.espresso.repubblica.it//pdf/Motivazioni_sentenza_Google.pdf.

11. *See, e.g.*, MGM Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 930 (2005) (explaining that one is liable "by intentionally inducing or encouraging direct infringement, . . . and infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it").

12. *See* 17 U.S.C. § 512 (2006).

13. One example of such a regime is the French HADOPI law, a graduated response system that terminates user Internet access after three strikes. *See French Downloaders Face Government Grilling*, BBC NEWS (July 27, 2011), http://www.bbc.co.uk/news/technology-14294517.

14. 17 U.S.C. § 512 (2006).

15. Digital Millennium Copyright Act, 17 U.S.C. §§ 101–1332 (2006).

16. *See, e.g.*, 17 U.S.C. §§ 108, 112(a), 117, 512, 1201 (2006).

Internet in the United States) do not have to comply with the DMCA's notice-and-takedown provisions.[17]

International law is fairly silent about intermediary liability, but it is unlikely to remain so for long. Earlier international trade treaties did not address intermediary liability. For example, the 1996 Agreement on Trade Related Aspects of Intellectual Property Law ("TRIPS Agreement") does not contain provisions concerning digital enforcement. This began to change with the adoption of the World Intellectual Property Rights Organization ("WIPO") Copyright Treaty, which contains language on technological protection measures[18] but not on intermediary liability regimes.[19] The EU addresses intermediary liability in the E-Commerce Directive[20] but lacks EU-wide criminal intermediary liability, because there is no EU-wide criminalization of copyright infringement.[21] If the European Parliament ratifies ACTA, this will change.[22] In the meantime, the United States has spread notice-and-takedown requirements to a number of countries through a series of bilateral free trade agreements[23] and appears to be trying to accomplish the same end through the TPP.[24]

17. *See* 17 U.S.C. § 512(a) (2006).

18. WIPO Copyright Treaty, *adopted* Dec. 20, 1996, arts. 11–12, S. Treaty Doc. No. 105–17, 36 I.L.M. 65 (providing legal remedies for violations of numerous "technological measures" and "rights management information" obligations such as distribution of material without authority and circumvention of effective technological measures protecting authors' rights).

19. *Id.*

20. Council Directive 2000/31/EC, ¶ 5, 2000 O.J. (L 178) 1 (EU) [hereinafter E-Commerce Directive] ("The development of information society services within the Community is hampered by a number of legal obstacles to the proper functioning of the internal market which make less attractive the exercise of the freedom of establishment and the freedom to provide services . . . .").

21. *See* 2010 O.J. (C 252) 7, 9 (implying that the European Commission decided to withdraw the proposal for an EU-wide criminal copyright law directive).

22. Kaminski, *Anti-Counterfeiting*, *supra* note 1, at 409.

23. Susan K. Sell, *The Global IP Upward Ratchet, Anti-Counterfeiting and Piracy Enforcement Efforts: The State of Play*, Program on Info. Just. Intell. Prop. Res. Paper Series, Paper No. 15 (2010), *available at* http://digitalcommons.wcl.american.edu/research/15/.

24. Sean Flynn et al., *Public Interest Analysis of the US TPP Proposal for an IP Chapter*, Program on Info. Just. Intell. Prop. Res. Paper Series, Paper No. 21

IV. FLEXIBILITY FOR INDIVIDUAL COUNTRIES: SOVEREIGNTY AND EXPERIMENTATION

Although the United States has been pushing for greater copyright protections in international law, it is not clear that cementing an international standard on intermediary liability is the right move at this time. Waiting to establish a standard based on principles, rather than specific requirements, would better respect the sovereignty of individual countries to choose whether to implement intermediary liability. Waiting would also afford countries flexibility for experimentation with different liability regimes to determine what policies work best in the long run. The Internet has not been around for very long, and prematurely standardizing one regime internationally will freeze experimentation. The effort to establish a single regime also assumes, incorrectly, that the international community shares one homogeneous understanding of the role of online intermediaries.[25]

It cannot be assumed that intermediaries should always be liable for user behavior. The experience of the United States sheds light on the complications inherent in establishing intermediary liability. Before the enactment of the Communications Decency Act ("CDA"), U.S. courts went back and forth over whether an online intermediary was liable for defamation, as a publisher would be,[26] or free from

(2011), *available at* http://digitalcommons.wcl.american.edu/research/21 (discussing the injunctive relief that would be allowed by article 12.2 of the TPP and consistent with its parallel provision, article 44 in TRIPS).

25. *See, e.g.*, LILIAN EDWARDS, ROLE AND RESPONSIBILITY OF INTERNET INTERMEDIARIES IN THE FIELD OF COPYRIGHT AND RELATED RIGHTS, WIPO (2011), *available at* http://www.wipo.int/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf (discussing the evolving understanding of intermediaries' role); Jeremy F. DeBeer & Christopher D. Clemmer, *Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?*, 49 JURIMETRICS J. 375 (2009) (comparing treatment of intermediaries in various jurisdictions around the world); Organisation for Economic Co-Operation and Development, *The Economic and Social Role of Internet Intermediaries* 1 (2010) (seeking to harmonize the definition of "intermediary").

26. *See, e.g.*, Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995) (noting that publishers are liable for defamatory content because they exercise editorial control and judgment).

liability, like a distributor.[27] The United States currently uses a statute to excuse online intermediaries from liability for users' defamatory statements.[28] However, courts have recognized a number of exceptions to this broad waiver of liability for online intermediaries. Intermediaries may be held liable if they encourage certain violations of the law. For example, the Ninth Circuit held that an intermediary could be held liable for providing a drop-down menu of discriminatory categories from which users could select when searching for roommates, a practice that violates the Fair Housing Act.[29] In the copyright context, a series of U.S. court cases recognized secondary liability for contributory or vicarious copyright infringement,[30] and the Supreme Court recognized intermediary liability for inducement of copyright infringement.[31] These exceptions to the general waiver of liability, as well as the concurrent ideas of secondary liability and inducement, took more than two decades to gain traction and become established law.

Thus, it is not a given that intermediaries are always liable for user behavior. U.S. courts continue to struggle with determining when an intermediary might be liable. Statutes and treaties that create "safe harbors" for intermediaries internationally are based on an implicit and unfounded assumption that law in different countries universally recognizes that intermediaries should be held liable for user behavior.[32] This is a tenuous position.

27. *See, e.g.*, Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991) (noting that distributors are not liable for defamatory content because they are considered passive conduits that generally do not monitor content).

28. *See* 47 U.S.C. § 230(c)(1) (2006).

29. *See* Fair Hous. Council v. Roommates.com, 521 F.3d 1157 (9th Cir. 2008) (en banc).

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

31. *See* MGM Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

32. *See* Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, 2000 O.J. (L 178) 1 (June 8, 2000); Electronic Commerce (E.C. Directive) Regulations, 2002, S.I. 2002/2013, regs. 17 (mere conduit), 18 (caching), 19 (hosting) (U.K.); *Regulation on Protection of the Right to Network Dissemination of Information*, COPYRIGHT PROT. CTR. OF CHINA, http://www.ccopyright.com.cn/cms/ArticleServlet?articleID=7641 (last visited July 18, 2012) (discussing liability in regards to access to information, providing storage space, and providing linking

Where intermediary liability does exist, there are legitimate reasons for crafting limitations on that liability. It may, in fact, make sense to standardize safe harbors to prevent overzealous content regulation and privacy violations. The Internet is international, and online providers such as Facebook operate internationally. It would be less costly to have one standard set of rules, under which companies can operate knowing they are in compliance with a number of countries' laws, rather than forcing those companies to adjust their behavior for every jurisdiction. The potential benefits of standardization are many: lower transaction costs, in the form of compliance checks, and greater willingness to expand into markets that share the standardized rules, among others.[33] However, it is very important that any standardized regime comprise a balanced set of rules that protect the interests of all of the parties affected by them, as discussed below.

V. RECENT TRENDS IN FREE TRADE AGREEMENTS

A number of trends concerning online intermediaries can be identified in the recent proposals for free trade agreements, such as ACTA and TPP. One troubling trend is the imposition of criminal liability on intermediaries for users' copyright infringement.[34] Another trend consists of encouraging businesses to make private deals with each other.[35] An example of this took place in the United

and searching services for works, performance, audio-visual recordings); Information Technology Act § 79, 2000, No. 21, Acts of Parliament, 2000 (India) (delineating cases where a network service provider would not be held liable for the actions of its users if it had no knowledge of the content on its network and, when it became aware of the content, exercised due diligence to rectify the violation); WIPO Copyright Treaty, *supra* note 18, art. 8.

33. JOHN H. JACKSON & WILLIAM J. DAVEY, LEGAL PROBLEMS OF INTERNATIONAL ECONOMIC RELATIONS 36 (2d ed. 1986 & Supp. 1989) (suggesting that transaction costs could be "minimized or eliminated if customs and practices could be standardized and made uniform throughout the world").

34. Kaminski, *Anti-Counterfeiting*, *supra* note 1.

35. *See id*. at 393; *see also* Annemarie Bridy, *ACTA and the Specter of Graduated Response*, Program on Info. Just. Intell. Prop. Res. Paper Series, Paper No. 2 (2010), *available at* http://digitalcommons.wcl.american.edu/research/2 (pointing out the "privately ordered graduated response" in the United States and Ireland despite the U.S. Trade Representative publicly announcing "no participant

States when a number of ISPs entered into a memorandum of understanding with content producers, agreeing to send warning notices to potentially infringing users, followed by "mitigation measures" that could include reductions of Internet speeds, redirection to a landing page, or other measures.[36] This privatized system amplifies the public choice and due process problems for users, who have no voice in the negotiations of private agreements and little to no say in whatever takedown process companies establish.

In negotiations for the Anti-Counterfeiting Trade Agreement, some countries pushed to establish "graduated response."[37] Graduated response refers to an incremental enforcement system, whereby intermediaries monitor users' content for copyright-infringing works, send infringing users notices and warnings, and eventually deny them access to the intermediaries' systems, if the infringement continues unabated. In the ACTA negotiations, the proposal to include graduated response failed, as a result of strong public opposition; it has not yet resurfaced in the TPP negotiations.[38] The U.S. proposal for digital enforcement in free trade agreements appears to resemble the Digital Millennium Copyright Act's system of notice-and-takedown. But, as I have discussed briefly elsewhere and will discuss below, the current proposals lack significant protections for users.[39]

VI. GENERAL PRINCIPLES

This section outlines the general principles that countries should keep in mind when negotiating intermediary liability.[40] It discusses the following general principles in no particular order. Although they

is proposing to require governments to mandate a 'graduated response'").

36. *See Frequently Asked Questions*, CTR. FOR COPYRIGHT INFO., http://www.copyrightinformation.org/faq (last visited July 18, 2012).

37. *See* Bridy, *supra* note 35.

38. *See id.* at 3–4; Alberto Cerda, *Right to Privacy in Trans-Pacific Partnership (TPP) Negotiations*, KNOWLEDGE ECOLOGY INT'L BLOG (June 19, 2011, 9:00 AM), http://keionline.org/node/1164 ("[B]ecause of the pressure of data privacy authorities of the European Union, ACTA gave up some of those controversial measures [such as the graduated response] . . . .").

39. Kaminski, *Plurilateral Agreements*, *supra* note 1.

40. *See* Zimmerman, *supra* note 2.

are interrelated, most can be adopted independently of one another.

1. *Be clear that provision of the safe harbors does not, in itself, establish intermediary liability.* In the DMCA, section 512(1) clarifies that compliance with notice-and-takedown does not affect the intermediary's ability to claim that its behavior is not, in the first instance, infringing.
2. *To protect user privacy, be clear about not establishing a duty to monitor user activity.* As discussed above, liability incentivizes intermediaries to monitor user activity.[41] Governments must make a clear statement that this behavior is not required. They could in fact add language prohibiting monitoring more generally. In the United States, the DMCA clarifies that liability safe harbors are not conditioned on intermediaries monitoring services, except to the extent consistent with a "standard technical measure."[42] More broadly, the E-Commerce Directive in the EU prevents member states from imposing on intermediaries a general obligation to monitor information that they transmit or store, regardless of their compliance with safe harbors.[43]
3. *Be careful not to define infringement too broadly.* An overly expansive definition of copyright infringement, such as one that includes temporary copies, may make intermediaries liable for direct infringement, rather than secondary infringement.[44] It also broadens liability for user-created content, because more of that user-created content will be considered infringing.

41. *See supra* Part II; *supra* notes 1–4 and accompanying text.
42. 17 U.S.C. § 512(m)(2) (2006).
43. E-Commerce Directive, *supra* note 20, arts. 12–14.
44. *Cf.* David Lindsay, *Copyright Infringement via the Internet: the Liability of Intermediaries*, CTR. FOR MEDIA, COMMC'NS & INFO. TECH. L. 17–22, 51–54, 68, 97–99 (2000), *available at* http://www.lawapps.law.unimelb.edu.au/cmcl/publications/Copy11.pdf (noting the difficulty Australian courts are having grappling with the issue of whether a digital version of a non-digital material constitutes a reproduction, and noting, in contrast, that in the United States, distribution of materials via computer networks infringes distribution rights).

4. *Be extremely cautious in implementing statutory damages.* Statutory, or "pre-established," damages establish huge financial penalties for copyright infringement, with no proof of actual damage required.[45] Aside from the risks that statutory damages create for users themselves, statutory damages incentivize intermediaries to take more material down, because the possible monetary loss they face is much higher.
5. *Avoid establishing criminal liability for third parties.* Criminal liability, or enforcement by the government rather than private actors, is a new idea in discussions of intermediary liability. In the United States, there is an open question as to what level of willfulness is required for secondary criminal liability, which U.S. case law does not yet address.[46] The danger of establishing criminal liability for third parties is that, in the absence of clear standards on willfulness or inducement, criminal liability establishes a shadow system of liability. Even if a company complies with civil safe harbor provisions, it may still be criminally liable. Thus, civil safe harbors will not prevent intermediaries from behaving in self-protective ways; these behaviors will persist in order to avoid criminal liability.
6. *Do not require intermediaries to terminate user Internet accounts in response to copyright infringement claims in the absence of court oversight.* The Internet has become the primary mode of communication and socialization for

45. Pamela Samuelson & Tara Wheatland, *Statutory Damages in Copyright Law: A Remedy in Need of Reform*, 51 WM. & MARY L. REV. 439, 441 (2009) (explaining that the United States is "an outlier in the global copyright community in giving plaintiffs in copyright cases the ability to elect, at any time before final judgment, to receive an award of statutory damages").

46. *See* David G. Robinson, *Following the Money: A Better Way Forward on the PROTECT IP Act*, Yale Law School, Info. Soc'y Project, Working Paper No. 1 (2011), *available at* http://www.law.yale.edu/intellectuallife/6564.htm (follow "Following the Money: A Better Way Forward on the Protect IP Act" hyperlink; then "One-Click Download" hyperlink) (discussing the impact of domain name seizures and the involvement of several enforcement agencies and the application of U.S. statutes, still noting the violation of First Amendment and Fifth Amendment rights).

most people.[47] Account termination is a disproportionate remedy for copyright infringement; it threatens that individual's right of free expression and ability to participate in many aspects of modern life. In evaluating an earlier version of France's graduated response law, the French Constitutional Court found that the law undercut free speech and the presumption of innocence; the court, therefore, established that enforcement of the law required court oversight.[48]

7. *Establish due process for users.* The most dangerous part of establishing intermediary liability safe harbors, such as the DMCA's notice-and-takedown provisions, is that the procedures often take place outside of the judicial system. A content owner can request a takedown of material, which may remain down for a significant amount of time, even if it is ultimately not infringing.[49] There are ways to better protect due process: Chile, for example, uses courts to determine whether material is infringing before intermediaries must take it down.[50]

8. *Give users the procedural ability to protest/sanction bad behavior.* This principle is related to the due process concern. Just as countries should make sure that there is enough judicial oversight for claims of infringement to allow users to protect their own rights, they can and should empower users to monitor the system in their own interest.

47. *See, e.g.*, Shanyang Zhao, *The Internet and the Transformation of Everyday Life*, 76 SOC. INQUIRY 458 (2006) (explaining how temporal and spatial structure of everyday life is expanded, including the ability of parties to communicate instantaneously over huge distances, the forging of relationships with others despite a lack of face-to-face meetings, and so on).

48. *See* Peggy Hollinger, *French Anti-Piracy Drive Ruled Illegal*, FIN. TIMES (June 11, 2009, 3:00 AM), http://www.ft.com/cms/s/0/986d8406-5620-11de-ab7e-00144feabdc0.html#axzz1mVyD6zKI.

49. *Cf.* Declan McCullagh, *DHS Abruptly Abandons Copyright Seizure of Hip-Hop Blog*, CNET (Dec. 8, 2011, 11:14 AM), http://news.cnet.com/8301-31921_3-57339569-281/dhs-abruptly-abandons-copyright-seizure-of-hip-hop-blog/ (indicating that ICE did not use "prior restraint" and that the government's claims were "exaggerated").

50. *Chile*, GLOBAL CENSORSHIP CHOKEPOINTS, https://globalchokepoints.org/countries/chile (last visited July 18, 2012).

One example is allowing users to sue overeager content owners who deliberately claim infringement where they know none exists, as is present in the DMCA section 512(f).[51]

9. *Leave flexibility for countries to experiment with broader user protections.* While intermediary safe harbors are good, any international agreement should leave flexibility for countries to establish systems that are more protective of users, such as Canada's notice-and-notice system[52] or Chile's decision to involve its court system in determining whether material is, in fact, infringing.[53]

10. *Include limitations and exceptions to the liability rules, such as fair use.* In the United States, the doctrine of "fair use" allows individuals to use portions of a copyrighted work for selected academic purposes or for other selected applications, such as parody, without a license.[54] Fair use is an affirmative defense to claims of copyright infringement and is crucial to protecting users' abilities to innovate using copyrighted works. In ACTA, there was no mention of fair use or limitations and exceptions, apart from the section on technological protection measures. In this section, ACTA permits parties to adopt or maintain appropriate limitations or exceptions to the implementation of technological protection measures.[55]

Many developing countries fail to implement the full scope of limitations and exceptions.[56] When negotiating free trade agreements,

51. 17 U.S.C. § 512(f) (2006).

52. Copyright Modernization Act, Bill C-11 § 47, 41st Parliament (2011–2012) (Can.).

53. *See* GLOBAL CENSORSHIP CHOKEPOINTS, *supra* note 50.

54. *See Frequently Asked Questions (and Answers)*, ELECT. FRONTIER FOUND., http://w2.eff.org/IP/eff_fair_use_faq.php (last visited July 18, 2012) ("Fair use allows consumers to make a copy of part or all of a copyrighted work, even where the copyright holder has not given permission or objects to your use of the work.").

55. Anti-Counterfeiting Trade Agreement, Dec. 3, 2010, art. 27.8 [hereinafter ACTA], *available at* http://www.dfat.gov.au/trade/acta/Final-ACTA-text-following-legal-verification.pdf.

56. CAROLYN DEERE, THE IMPLEMENTATION GAME: THE TRIPS AGREEMENT AND THE GLOBAL POLITICS OF INTELLECTUAL PROPERTY REFORM IN DEVELOPING

these countries must be sure to include explicit mention of exceptions and limitations. Otherwise, these protections likely will not make it into domestic law, and intermediaries will, consequently, be left liable for more types of user behavior.

VII. BALANCING PROVISIONS FOR NOTICE-AND-TAKEDOWN REGIMES

It is not clear whether notice-and-takedown should become the international standard. However, if it is going to be considered, there are important balancing mechanisms that should be included to protect Internet users. This section explores in greater detail the types of balancing provisions that should be included in free trade agreements if they are to include notice-and-takedown regimes.

A. NOTIFYING USERS WHEN MATERIAL IS TAKEN DOWN

Users should be notified when their content is taken down. Otherwise, their speech rights will be threatened without giving them an opportunity to respond. In U.S. law, the intermediary is incentivized to take reasonable steps to "promptly" notify users when it has removed material; otherwise, the intermediary can be liable to users for taking material down.[57] This allows a user who is invested in the particular speech to know about and potentially protest its removal. International agreements could, additionally, include an outside window for notifying users to ensure that intermediaries are spurred to contact users as soon as possible, instead of leaving the precise time period at the discretion of individual countries.

B. COUNTER-NOTICE, OR COUNTER-NOTIFICATION

Users should have the ability to respond to claims of infringement and to request that an intermediary put material back up. In U.S. law, the intermediary must replace removed material in ten to fourteen business days, following the receipt of the counter-notice. If the intermediary fails to do so, it may be liable to the user for having removed the material in the first place.[58] The free trade agreements in

COUNTRIES 203 (2008).

57. 17 U.S.C. § 512(g)(2)(A) (2006).

58. *See* 17 U.S.C. § 512(g)(2)(C) (2006).

question lack concrete timelines for restoring material, referring only to "a reasonable time."[59] On the one hand, this may allow countries the flexibility to implement a shorter timeframe. On the other hand, if countries directly adopt the language of the free trade agreements, this allows intermediaries to sit on counter-notifications for a longer time with no consequences. Note that the ten days of required removal time in the United States after receipt of the counter-notice is a long time for legitimate material to remain down if it is, in fact, not infringing.[60]

C. SANCTIONS FOR KNOWING MISREPRESENTATION

Notice-and-takedown regimes that occur outside of a court run a strong risk of abuse by those people requesting takedowns, since no court is required to establish that the material is, in fact, infringing before it is taken down. To counter this potential for abuse, the DMCA contains a provision in section 512(f) that establishes liability for making material misrepresentations that content is infringing when the claimant knows that it is not infringing. This prevents abuse of the notice-and-takedown system for other kinds of censorship. The proposed language in ACTA, however, failed to include these sanctions.[61] Free trade agreements have included them, but they lack clarification that damages should include costs and attorneys' fees and that the intermediary can also sue for damages (in addition to the user whose material is taken down).[62]

D. SUBPOENAS FOR USER IDENTITY

Subpoenas that ask intermediaries to identify their users are a part

59. *See* Trade Promotion Agreement, U.S.-Colom. art. 16.11.29(b)(x), Nov. 22, 2006 [hereinafter U.S.-Colom. TPA], *available at* http://www.ustr.gov/webfm_send/1336; Trade Promotion Agreement, U.S.-Pan. art. 15.11.27(b)(x), June 28, 2007 [hereinafter U.S.-Pan. TPA], *available at* http://www.ustr.gov/sites/default/files/uploads/agreements/fta/panama/asset_upload_file131_10350.pdf; Trade Promotion Agreement, U.S.-S. Kor. art. 18.10.29(b)(x), June 30, 2007 [hereinafter U.S.-S. Kor. TPA], *available at* http://www.ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file273_12717.pdf.

60. *See* 17 U.S.C. § 512(g)(2)(B)-(C) (2006).

61. *See* Kaminski, *Anti-Counterfeiting*, *supra* note 1, at 439.

62. *See, e.g.*, U.S.-Colom. TPA, *supra* note 59; U.S.-Pan. TPA, *supra* note 59; U.S.-S. Kor. TPA, *supra* note 59.

of negotiations on intermediary liability. ACTA recommends that parties give officials the authority to require online service providers to disclose the identity of allegedly infringing users to rights holders.[63] There are substantial privacy and free speech concerns when accusers can obtain the identity of alleged infringers without due process or adequate proof of infringement. If a regime does not require that a claimant show infringement as a prerequisite to obtaining an Internet user's identity, the accuser could ostensibly use the process to find out anybody's identity, including whistleblowers or other people whose views the accuser dislikes.

In the United States, a court standard has developed that protects the anonymity of speakers in defamation cases and other lawsuits. That standard requires reasonable efforts to notify the accused Internet users that they are about to be identified; identification of the exact actions that constitute an actionable cause; allegation of the cause of action and sufficient evidence to survive a motion for summary judgment; and a court judgment, balancing the right of anonymous free speech against the strength of the case and the necessity for disclosure of identity in order for the plaintiff to proceed.[64]

The standard for an identifying subpoena in copyright law is lower and is, notably, in tension with the standard for anonymous speech elsewhere in U.S. law.[65] U.S. copyright law contains a provision allowing content owners to get a subpoena to obtain a user's identity from an intermediary without litigation—which means without establishing a case of infringement.[66] However, the DMCA and U.S. case law restrict use of this subpoena through provisions that are missing from free trade agreements. First, U.S. courts have found that

63. *See* ACTA, *supra* note 55.

64. *See, e.g.*, Dendrite Int'l, Inc. v. Doe No. 3, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001) (denying a discovery request because plaintiff failed to show any harm caused by the defamatory statement posted on a message board).

65. *See* Eric Goldman, *Did a Court Eliminate 512(h) Subpoenas?—Maximized Living v. Google*, TECH. & MKTG. L. BLOG (Jan. 6, 2012, http://blog.ericgoldman.org/archives/2012/01/did_a_court_eli.htm (discussing how the court made a distinction between "current infringing activity" and "former infringing activity," explaining that once the infringement no longer exists, subpoena power under 512(h) is quashed).

66. 17 U.S.C. § 512(h) (2006).

the subpoena for identifying information does not apply to neutral conduits, such as ISPs; these neutral conduits are excused from having to identify their users before a lawsuit has been filed.[67] Second, the DMCA requires that, even where section 512(h) subpoenas may be used, the accuser must include in its request for a subpoena a copy of an effective notification and a sworn declaration that "the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title."[68] This limits potential abuse of the subpoena by requiring its requestor to promise not to abuse it.

E. PRIVACY PROTECTIONS

The previous section discussed the necessity of including a provision clarifying that safe harbors should not be conditioned on monitoring users. U.S. law contains a second level of protection, but this protection is left out of free trade agreements. Under section 512(m)(2) of the DMCA, in order to avail itself of the safe harbor, an intermediary need not access material when that behavior is "prohibited by law."[69] The 1998 U.S. Copyright Office Summary of the DMCA explained that this provision prevents service providers from violating U.S. wiretap law, thereby prioritizing privacy over copyright enforcement—in accord with the ECJ's recent finding that user rights take priority over filtering for infringing behavior.[70]

67. *See, e.g.*, *In re* Charter Commc'ns, 393 F.3d 771 (8th Cir. 2005) ("[A] judicial subpoena is a court order that must be supported by a case or controversy at the time of its issuance.").

68. 17 U.S.C. § 512(h)(C) (2006).

69. 17 U.S.C. § 512(m)(2) (2006).

70. *European Court of Justice Rejects Web Piracy Filter*, BBC NEWS (Nov. 24, 2011), http://www.bbc.co.uk/news/technology-15871961 (discussing how the injunction "could potentially undermine freedom of information"); *see also* Case C-360/10, Belgische Verening van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV (Feb. 16, 2012), *available at* http://curia.europa.eu/juris/document/document.jsf?text&docid=119512&pageIndex=0&doclang=EN&mode=req&dir&occ=first&part=1&cid=158253 (explaining "national authorities and courts must strike a fair balance between the protection of copyright and the protection of the fundamental rights of individuals who are affected by such measures").

F. INJUNCTIONS

Injunctive relief refers to a court order requiring the intermediary to undertake an action, such as blocking access to infringing material. Because injunctive relief can interfere with speech, the DMCA requires a court to consider four factors when awarding injunctive relief: the burden to the intermediary; the harm to the copyright owner; whether the injunction is technically feasible and doesn't interfere with access to noninfringing material; and whether less burdensome, but equally effective, responses exist.[71] In contrast, the free trade agreements fail to ask courts to look to the potential combined burden to the intermediary from multiple injunctions. The DMCA also requires consideration of, not only whether an injunction is technically feasible and effective, but also whether it will interfere with access to noninfringing material on other online locations. This provision is missing from the free trade agreements and could adversely affect sites like search engines.

G. TERMINATING REPEAT-OFFENDER ACCOUNTS

The public response to ACTA turned negative when it was revealed that negotiators considered including language addressing the termination of the accounts of repeat offenders.[72] On its surface, this language resembles graduated response. Ultimately, it was not included in ACTA's final text.

U.S. law includes language requiring service providers to establish a policy for the termination of the accounts of repeat infringers.[73] However, the case law in the United States is mixed with regard to defining what constitutes a "repeat infringer"—whether the offense must have been found in court or merely identified by the content owner.[74] Negotiators should be cautious about including this

71. 17 U.S.C. § 512(j)(2) (2006).

72. *See, e.g.*, Paul Meller, *EU Data Protection Chief Slams ACTA Talks*, PC WORLD (Feb. 22, 2010, 5:00 AM), http://www.pcworld.com/article/189922/eu_data_protection_chief_slams_secret_acta_talks.html (noting the argument of civil liberty groups and academics that ACTA negotiations should not be held in secret because of the agreement's potential effect on Internet users worldwide).

73. *See* 17 U.S.C. § 512(i)(1) (2006).

74. Bridy, *supra* note 35, at 12 (illuminating how major broadband providers reserve the right to terminate access for repeat infringers in order to conform with section 512(i) of the DMCA).

language internationally because it could potentially create a system whereby users can have their Internet access disabled without a means to protest the disablement in court. At least one country has found this to be a violation of the rights guaranteed by its constitution.[75]

H. STANDARD TECHNICAL MEASURES

Both U.S. law and free trade agreements contain references to "standard technical measures" that intermediaries must accommodate.[76] However, in the DMCA, such measures must, by law, be developed pursuant to a broad consensus between copyright owners and service providers in an "open, fair, voluntary, multi-industry standards process."[77] They also must not impose substantial costs on service providers or substantial burdens on their systems or networks.[78] If free trade agreements are going to include references to standard technical measures, they must include multi-industry participants or risk that such measures will be set by copyright owners alone. They also should include references to the costs to and burdens on intermediaries.

VIII. CONCLUSION

This paper has attempted to outline both general principles and specific proposals for ensuring that users are protected when governments establish intermediary liability. Again, we should be cautious in rushing to establish international intermediary liability, given that diversity in the short run may result in a better system down the line. However, if the question of standardizing intermediary liability laws is brought to the negotiating table, the above considerations should be taken into account.

75. *See* Hollinger, *supra* note 48 (describing French court statement that Internet access is an implied right that can only be denied by a judge).

76. *See* Digital Millennium Copyright Act, 17 U.S.C. §§ 101–1332 (2006); *see also* Trans-Pacific Strategic Economic Partnership Agreement, June 3, 2005, *available at* http://www.sice.oas.org/Trade/CHL_Asia_e/mainAgreemt_e.pdf.

77. 17 U.S.C. § 512(i)(2)(A) (2006).

78. *Id.*