Electronic Frontier Foundation

BRIEFING PAPER: INTERNET SERVICE PROVIDER SAFE HARBORS AND EXPEDITED SUBPOENA PROCESS IN THE U.S. DIGITAL MILLENNIUM COPYRIGHT ACT AND RECENT BILATERAL FREE TRADE AGREEMENTS

A. INTRODUCTION

The U.S. Trade Representative is seeking to incorporate provisions in bilateral free trade agreements regulating the liability of Internet service providers ("ISPs") for copyright infringement that are modeled on similar provisions in the U.S. Digital Millennium Copyright Act ("DMCA").[1] U.S. rightsholders have sought these provisions in recent trade agreements to ensure that ISPs will assist in enforcing copyright. They claim that the provisions are necessary to provide U.S. rightsholders with "effective action against any act of infringement" of copyright under Article 41 of the Agreement on Trade-Related Aspects of Intellectual Property.[2]

The U.S. provisions do two main things:

> (1) they provide a limited immunity from copyright liability for ISPs who meet procedural requirements in four types of activities (the so-called "safe harbors"); and
> (2) require ISPs to disclose the identity of their subscribers upon receipt of a subpoena alleging copyright infringement (the "expedited subpoena").

While these safe harbor provisions purport to limit ISP liability, in practice in the U.S., they have increased the burdens on ISPs and diminished rights of Internet users. Moreover, they embed into the law a suggestion that absent the safe harbor, ISPs would be liable for otherwise blameless conduct. For ISPs in trading partner countries that would not have liability under national law, these provisions may therefore effectively create a presumption of liability where none exists. More importantly, recent free trade agreement ISP provisions are so complex and detailed that they remove all policy flexibility for trading partners seeking to develop domestically appropriate ISP incentive structures.

There are sound public policy reasons for granting true immunity to Internet Service Providers for certain services and activities. ISP immunity from digital copyright infringement directly fosters the expansion of the Internet and thus facilitates access to knowledge and culture. In addition, in many situations, consumers and students access the Internet though their local library or college, so providing limited immunity to these types of service providers directly supports education.

However, the U.S. safe harbor provisions do not provide a good model to follow. First, the U.S. provisions are a response to particular U.S. caselaw on secondary copyright liability that may not have any parallel in trading partner's national law. Second, there are numerous deficiencies with the U.S. provisions:

- the structure of the safe harbors leads ISPs to err on the side of restricting their users' activities, chilling much lawful, non-infringing online speech;
- the safe harbor provisions are based on an outdated technological framework that does not account for peer-to-peer file-sharing technology and the current architecture of the Internet. This has led to distorted use of the provisions and inappropriate efforts by rightsholders to terminate users' Internet access on the unproven allegation of copyright infringement;

---

[1] For instance, see U.S. –Singapore FTA, Article 16.9(22); U.S.-CAFTA, Article 15.10(27); U.S.-Chile FTA, Article 17.11(23).

[2] See Preamble U.S. – Australia FTA, Article 17.11(29).

- the U.S. notice and takedown procedure contains insufficient procedural safeguards and has been used as a tool of censorship by private parties such as the Church of Scientology, and the electronic voting machine manufacturer Diebold, Inc, to silence legitimate criticism;
- The safe harbor provisions have been too narrow to assist some online service providers and do not cover all relevant activities of online and Internet service providers and other Internet intermediaries;
- the scope of the immunity granted by the safe harbor provisions is unclear, as demonstrated by a set of conflicting cases; and
- the expedited administrative subpoena provision has been widely criticized for its deficiency of procedural due process and inadequate privacy protection.

Following, for the benefit of countries considering implementing such provisions, is a discussion of the background and problems experienced with the U.S. provisions, including drafting suggestions based on U.S. caselaw.

B. U.S. SAFE HARBOR PROVISIONS

Four Safe Harbors

Section 512 of the U.S. copyright legislation limits ISPs' copyright liability in certain circumstances for four activities:

(1) transitory communication of digital information (section 512(a));
(2) intermediate and temporary caching (section 512(b));
(3) hosting of an end-user's material on a network or ISP's system (section 512(c)); and
(4) provision of information location tools, such as hyperlinks (section 512(d)).

Compliance with the safe harbors in section 512 is not mandatory. An ISP that does not come within the safe harbors is not automatically liable for copyright infringement. Instead, infringement must be proven on general principles (section 512(n)).

Limited Immunity

An ISP that comes within the safe harbor provisions obtains immunity from monetary penalties from copyright holders and from all but very limited forms of injunctive relief for secondary copyright infringement . Since the DMCA was enacted in 1998, no ISP that has qualified for the safe harbors has been subject to monetary damages or injunction.

Qualifying Conditions

In order to obtain the limited immunity, ISPs must comply with various conditions. For all the subsections, ISPs must adopt and reasonably implement a policy that provides for termination, in appropriate circumstances, of ***"repeat infringers"*** (section 512(i)). In addition, the third and fourth safe harbors also require ISPs to remove or block access to material residing on their system upon receipt of an appropriate "takedown" notice from a rightsholder or an authorized agent of a rightsholder.

C. BACKGROUND TO U.S. PROVISIONS

The U.S. ISP industry sought "safe harbors" to obtain immunity for ISP activities for two reasons.

(a) to remove legal uncertainty following two conflicting American cases on whether ISPs could be liable for their users' activities: *Religious Tech. Center v. Netcom On-Line Communication Services Inc.*, 907 F. Supp. 1361 (N.D.Ca Dist Crt, 1995) and *Playboy Enterprise Inc. v. Frena*, 839 F. Supp 1552 (M.D. Fla. 1993). These decisions involved

the U.S secondary copyright liability doctrines of contributory copyright infringement and vicarious liability; and

(b) to protect themselves against liability for temporary reproduction of copyrighted works in computer memory, following a controversial U.S. government taskforce report that claimed that these temporary reproductions were actionable copyright infringement, for which ISPs would be strictly liable.[3]

The scope and content of the safe harbor provisions reflect the particular American cases which they sought to clarify. For instance, section 512(a) reflects the U.S. Congress' decision to follow the *Religious Tech. Center v. Netcom On-Line Communication Services Inc*., decision and reject the *Playboy Enterprise Inc. v. Frena* decision. In addition, the conditions in section 512(i) of the U.S. copyright legislation that all ISPs must satisfy to qualify for the safe harbors reflect the elements of two secondary liability doctrines that are unique to U.S. jurisprudence: vicarious liability and contributory copyright liability.

D. Policy Issues and Problems in Operation

1. Since the safe harbor provisions reflect particular U.S. case law, harmonization with U.S. law may actually result in ISP liability where none currently exists.

The U.S. provisions are designed to harmonize trading partners' law with America's law on secondary copyright liability. While this benefits U.S. rightsholders who will be able to utilize a familiar set of laws, harmonization is inappropriate in this area because it ignores other countries' different legal principles and caselaw. The U.S. provisions are a response to particular U.S. caselaw that caused American ISPs to believe that they may have had liability for copyright infringement. In countries where ISPs would not have liability, U.S.-style safe harbor provisions are not necessary and will not provide any *real* protection. As a result, adopting provisions purporting to *limit* ISP liability may actually do the reverse; it may implicitly create a basis for ISP liability where none would exist. This is consistent with the U.S. copyright industry's public statements that the inclusion of similar provisions in the U.S.- Singapore free trade agreement required the introduction of a system of ISP liability.[4]

The U.S. safe harbors were arguably unnecessary in the U.S.[5] and are even less likely to fit with the differing copyright regimes of U.S. trade partners. There is no common agreement in international law as to the existence or content of a secondary copyright liability. Moreover, the second motivating factor, the National Information Infrastructure Task Force Working Group's view of temporary reproduction, was controversial within the United States when announced in 1995 and subsequent efforts to have it adopted at the international level were flatly rejected. The Chair of the U.S. NII Working Group put forward a provision that temporary reproductions in computer memory were actionable reproductions in the diplomatic conference leading up to the

---

[3] *Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights* (1995) (NII White Paper), at pages 65-66; 100, footnote 315, interpreting *Mai Systems v. Peak Computer,* 1992 US Dist. LEXIS 21829 (C.D.Cal. 1992), aff'd 991 F.2d 511 (9th Circ. 1993), and 122 on liability. See Prof. Jessica Litman, *Digital Copyright* (Prometheus Books, 2001), pp.91-96 for discussion of the U.S. Information Infrastructure Task Force, *Intellectual Property and the National Information Infrastructure: A Preliminary Draft of the Report of the Working Group on Intellectual Property Rights* (1994) (the Green Paper) pp.35-37, and the NII White Paper. See Litman, op cit, p.129.

[4] Report of the Industry Functional Advisory Committee Report on Intellectual Property on the U.S.-Singapore free trade agreement, 28 February 2003, page19, available at: http://www.ustr.gov/new/fta/Singapore/advisor_reports.htm
"The only concern is to ensure that, in implementing the "limitations" on liability provided in the agreement, Singapore also ensures that it has in place a system of liability of ISPs in the first place.."

[5] See Litman, op cit, chapter 9.

1996 WIPO Copyright Treaty. Reflecting the lack of international agreement on this issue, that Article was rejected.[6] Notwithstanding the lack of international agreement on this point, provisions stating that temporary reproductions in electronic form are actionable copyright infringement have been included in recent United States' bilateral and regional free trade agreements.[7]

Although the safe harbor provisions were nominally intended to benefit ISPs by clarifying when they did not have liability, in the U.S. they have instead been used to push for a de facto liability standard and have imposed a significant cost burden on ISPs with little or no commensurate benefit. The limitations of liability only apply if an ISP's conduct would give rise to liability under *existing* law and if the ISP meets the conditions in section 512.[8] However, U.S. copyright holders have filed briefs in lawsuits asking the Court to treat an ISP's non-compliance with the statutory safe harbor conditions as prima facie evidence of copyright liability.[9] Thus, instead of easing the pressures and scrutiny of ISPs, section 512 has increased their risks, costs, and burdens in dealing with copyright liability on the Internet.

This is likely to be repeated at the international level. Although the provisions purport to limit ISPs' liability, in practice, they are likely to expand it. U.S. rightsholders are seeking to have these provisions adopted in trading partners' laws to ensure that ISPs undertake particular enforcement activity in exchange for the safe harbor. Thus, the focus of these provisions is on enforcement of copyright by ISPs, not the creation of ISP immunity.

2. The notice and takedown procedure is particularly susceptible to abuse and has imposed a significant cost burden on U.S. ISPs with little, or no, commensurate benefit to consumers or the ISP community

These provisions have been misused by private parties to censor legitimate criticism, rather than to protect intellectual property. For instance, in 2003, after much public criticism about the performance of their electronic voting machines, Diebold, Inc., a U.S. manufacturer of electronic voting machines, issued a series of copyright takedown notices to numerous ISPs, demanding that they take down websites that hosted email messages from Diebold employees. Diebold also sent takedown notices to websites that *linked* to websites that hosted the email archive. A number of the email messages disclosed serious flaws with the company's electronic voting machines which were to be used in many American states in the upcoming November 2004 U.S. election.

The email archive was released on to the Internet by an unknown person in September 2003. Subsequently, two students hosted it on their website. That website was linked to by the website of IndyMedia, a network of independent journalists. Diebold sent takedown notices to

---

[6] *Basic Proposal for the Substantive Provisions of the Treaty on Certain Questions Concerning the Protection of Literary and Artistic Works to be Considered by the Diplomatic Conference*, Article 791), WIPO Doc. CRNR/DC/4, August 30, 1996. See Litman, op cit, p.129, and Agreed Statement to Article 1(4) of WIPO Copyright Treaty of 1996.

[7] For instance, see U.S.-CAFTA, Art. 15.5(1); U.S. – Australia FTA, Art. 17.4(1); U.S. – Singapore FTA, Art. 17.5(1), all available from www.ustr.gov.

[8] See Conference Report of the U.S. House of Representatives and Senate, 105th Cong., 2d, H. Report 105-796, at p. 73: "Section 512 is not intended to imply that a service provider is or is not liable as an infringer either for conduct that qualifies for a limitation of liability or for conduct that fails to so qualify."; House Commerce Committee H. Report, 105th Cong., 2d, Report 105-551, Part 2, at p.50; Senate Judiciary Committee Report, 105th Cong. 2d, S. Report 105- 190, at p.19.

[9] See Amicus Curiae brief filed by the Recording Industry Association of America in *CoStar Group Inc. v. LoopNet,* Case No. 03-1911 in 7th Circuit Court of Appeals, filed 22 October 2003 at p. 2, 15. See Defendants' Opposition to Motion for Preliminary Injunction, in *Online Policy Group ct al v. Diebold, Inc.,* (N.D.Ca Dist. Crt, Case No. 03-4913 JF) at p. 20.

Swarthmore College (which served as the students' ISP), and to Online Policy Group (OPG), which hosted the IndyMedia group's website. In each case, Diebold demanded the removal of the emails or links to them, threatening copyright liability if they did not comply. Swarthmore complied by requiring the students to remove the materials from their educational website. When OPG resisted, Diebold sent further takedown notices to OPG's upstream ISP, demanding the termination of the downstream "infringing" users.

EFF with co-counsel, the Stanford University Law School's Center for Internet and Society Cyberlaw Clinic, brought a lawsuit under the "knowing material misrepresentation" provision in section 512(f) of the U.S. copyright law on behalf of the students and OPG. The lawsuit argued that Diebold was misusing the copyright takedown provisions to censor material that was covered by "fair use" under U.S. law - political commentary on a matter of high public importance - and that Diebold had misrepresented that there was copyright infringement in order to remove emails that reflected badly on its products. The court agreed[10] and Diebold settled by paying damages.

In the vast majority of cases, however, an ISP is not likely to investigate the validity of a purported takedown notice, or expend resources to obtain clarification of its legal obligations, and the operator of the removed website will not have the resources to challenge the takedown. The DMCA provisions give ISPs the incentive to take down first, and ask questions (if at all) later. As a result, the takedown provisions effectively act to censor much speech on the basis of a mere claim of infringement by a private party.

The Church of Scientology has also used copyright takedown notices to silence its critics. This has been particularly successful against critics that reside outside of the United States because of a limitation in the DMCA's counter-notification process. The Church issued a takedown notice to a U.S.-based ISP to remove a website that it was hosting that was critical of the Church's teachings.[11] The website's authors resided outside of the United States. Although they believed the copyright infringement claim was false, they were not able to issue a counter-notice, to have the website restored, because that would have required them to agree to the jurisdiction of U.S. courts, which was not appropriate given their location.

The Church of Scientology has sent dozens of takedown notices to the popular Internet search engine, Google, demanding that it remove links to certain websites that are critical of the Church when it displays search results for 'Scientology". Thus, the Church of Scientology has successfully used the DMCA notice and takedown provisions to prevent Google users from finding criticism about the Church. This has directly impaired access to knowledge and freedom of speech online. Google also routinely receives takedown demands with tenuous copyright claims from online merchants who want their competitors removed from the search engine. If Google and other search engines accede to these requests, consumers' access to a fair marketplace is diminished.[12]

The notice and takedown process has largely been automated through the use of "bots" which scan the Internet for potentially infringing material. Unfortunately this has led to notices being issued with little, if any, human review. Copyright owners have issued takedown notices for material that is in the public domain (and hence not copyrighted), for a child's book report about

---

[10] *Online Policy Group, Nelson Chu Pavlosky and Luke Thomas Smith* v. *Diebold, Inc. and Diebold Election Systems, Inc.,* (N.D. Ca, Case No. C 03-04913, September 30, 2004), available at: <http://www.eff.org/legal/ISP_liability/OPG_v_Diebold/20040930_Diebold_SJ_Order.pdf>

[11] Declan McCullagh, "Google Yanks Anti-Church Sites," Wired News, Mar. 21, 2002 <http://wired.com/news/politics/0,1283,51233,00.html>

[12] *See* DMCA demands sent to Google at <http://www.chillingeffects.org/dmca512/keyword.cgi?KeywordID=2>.

"Harry Potter", for a family photo of a "Mrs. Harrison" (no relation to former Beatle George Harrison) and for a song written by a professor of astronomy with a similar name to a popular recording artist.[13] Section 512(c)(3) requires the copyright owner to state that he or she has a "good faith" belief of infringement. However, it does not require any investigation as to whether there is actual infringement.[14]

The misuse of takedown notices might be addressed by requiring that any takedown notice be reviewed by a judge or a special government agency, or alternatively, by adopting an appropriately-tailored "notice and notice" regime such as that recently proposed by Canada in place of a takedown regime,[15]

3. **These provisions are not a sound policy solution to the perceived problem because they are based on specific, outdated technology and do not provide a sufficiently flexible basis for regulating fast-evolving technologies**

The U.S. provisions were created in 1997 before peer-to-peer file-sharing technology was in widespread use. As a result, they do not account for file-sharing activity, the fastest-growing sector of Internet use. In the U.S. it is estimated that tens of millions of Americans regularly use peer-to-peer software to share music or video files, video games or computer software. Since 2003 the U.S. music industry has filed over 10,000 lawsuits against individuals for alleged copyright infringement due to file-sharing.

The key feature of current peer-to-peer software technology is that Internet users who have installed such software can connect to one another directly (peer to peer) without relying on any central index or service. When a user downloads a song or movie that he or she has found with file-sharing software, it is downloaded directly from one individual to another. Usually, the only role played by the ISP is providing a connection to the Internet. The packets of data that comprise the music or audio file pass across the ISP's network, but neither the individual packets, nor the complete music file is stored on the ISP's network or computer system.

In cases where ISPs simply provide Internet connectivity, they would usually fall within the first safe harbor for transitory communications, in section 512(a). To avail themselves of that safe harbor, ISPs must have implemented a policy of terminating subscribers who are *"repeat infringers"*. However, in an effort to use ISPs for enforcement, U.S. copyright holders have sent ISPs thousands of inappropriate section 512(c) *takedown notices* to force ISPs to terminate their subscribers upon the mere *allegation* of copyright infringement.

The safe harbor for webcasting in section 512(c) provides ISPs with immunity where ISPs remove or block access to particular material hosted on their system when they have actual knowledge or receive a takedown notice alleging that the material is copyright-infringing. The takedown notice procedure relies on the ISP having control over material residing on the ISP's system or network. However, it does not make sense when applied to peer-to-peer architecture, where allegedly copyright-infringing material resides on end users' computers over which the ISP has no control, rather than on the ISP's network or system.

The webhosting safe harbor was not designed to cover the peer-to-peer situation. This misapplication of the takedown notice provisions to deal with an unforeseen situation has increased the level of legal uncertainty for all stakeholders. For instance, ISP Pacific Bell Internet Services complained that the enforcement agent of the Recording Industry Association of

---

[13] See *Unsafe Harbors – Abusive DMCA Subpoenas and Takedown Notices*, EFF report on section 512, at http://www.eff.org/IP/P2P/20030926_unsafe_harbors.php and http://www.chillingeffects.org

[14] See *Rossi v. Motion Picture Association of America*, 67 U.S. P. Q. 2d 1047 (D. Haw. 2003).

[15] *See* <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/en/rp01142e.html>

America, MediaForce, sent the ISP over 16,700 arguably invalid "takedown" notices under section 512 (c) of the U.S. Copyright statute, requesting it to "remove" copyrighted material which the ISP's subscribers had allegedly downloaded on to their computers from file-trading networks.[16] Other large ISPs, like Verizon, have experienced similar difficulties. The growing misuse of takedown notices recently led a U.S. Congressman to call for a Congressional investigation into this practice.[17]

In addition, some rightsholders have been delivering thousands of "termination notices" to ISPs, arguing that mere allegations of infringement are enough to trigger the "termination of repeat infringers" obligation contained in 512(i). If this were the law (and many ISPs do not believe it is), private parties would be able to cut individuals off from Internet access altogether, based on a simple, unproven allegation of infringement.

Since these provisions are sourced in an international legal agreement, they will be more highly entrenched than routine domestic legislation. It will be difficult to change these provisions because any change to domestic legislation would likely require a corresponding change to the international trade agreement that underpins them. It is more likely that stakeholders will seek to reinterpret the existing obligations to accommodate changes to technologies and system functionality. In turn, this is likely to result in a distortion of the operation of these provisions, and a correspondingly greater level of uncertainty about liability for all stakeholders, as courts attempt to stretch the provisions to new technologies and network functions that were not foreseen at the time of the agreement, such as peer-to-peer technology. This is likely to impede investment in new technology and innovation and increase costs for consumers who wish to utilize new technologies.

4. Termination of Internet access on the allegation of copyright infringement - the "Repeat Infringer" Problem

U.S. copyright holders have convinced some ISPs to terminate subscribers' Internet access on the basis of a mere allegation of copyright infringement, even though there is no legal obligation to do so.

All of the four U.S. safe harbors are conditioned on the ISP having adopted, and reasonably implemented, a policy of terminating "repeat infringers" (section 512(i)). The Act does not define "repeat infringers" and no case has been brought on this point yet. Although many U.S. legal scholars,[18] have argued that ISPs do not have any legal obligation to terminate upon a mere allegation of copyright infringement, U.S. rightsholders have continued to ask ISPs to terminate subscribers based on a single notice alleging copyright infringement on a peer-to-peer file-sharing network.[19] As a result, Internet users' ability to access the Internet is threatened by automated notices from private parties that often contain errors.

---

[16] *Pacific Bell Internet Services v. Recording Industry Association of America, Inc et al,* (U.S. District Court, Northern District of California, San Francisco Division, Case No. C 03-3560 SI).

[17] Letter from Rep. Dennis Kucinich to House Judiciary Committee, 21 November 2003, requesting investigation of abuse of section 512 notices: http://www.house.gov/kucinich/issues/Jud-Cmte-Invstgn.pdf

[18] David Nimmer, *Repeat Infringers*, 52 JOURNAL OF THE COPYRIGHT SOCIETY OF THE U.S.A. 170 (WINTER 2005).

[19] In a presentation in Australia in 2004, the Vice President and Associate General Counsel of Verizon Communications, Inc., Sarah Deutsch, noted that one small U.S. ISP had received over 20,000 notices in 2003 and all were invalid peer-to-peer notices asking for termination of subscribers. Before the shift to automated search bots, the same ISP received under 1000 notices a year. Another US ISP received over 30,000 notices from January through April 2004 alone- only 2 of which were legitimate takedown notices. In the previous 12 months, the same ISP received over 90,000 invalid peer-to-peer notices. As Ms. Deutsch

This could be redressed either by removing any obligation to terminate and allowing rightsholders to rely on the existing injunction power in section 512(j), or by conditioning the ISP termination obligation in subsection 512(i) on being served with a court order requiring termination of an identified subscriber for proven second or subsequent infringement.

E. EXPEDITED SUBPOENA PROCESS

Section 512(h) of the U.S. Copyright statute creates an expedited administrative subpoena process that permits copyright holders to direct ISPs to disclose the identities of their subscribers, on a mere allegation of copyright infringement. The expedited subpoena process permits court clerks to issue subpoenas directing ISPs to disclose the name and contact information for an ISP's subscriber, upon a "good faith" allegation of copyright infringement by a purported copyright owner. Upon receipt of a subpoena, an ISP must provide the copyright owner with the subscriber's identity "expeditiously".

Many of the problems experienced in the United States arose out of the administrative character of the expedited subpoena and the low threshold of required proof of infringement. Unlike U.S. section 512(h), the ISP provisions in the United States' recent bilateral free trade agreements leave open the possibility of *a judicial* process to obtain such subpoenas. This would avoid many of the U.S. problems. (For instance, see U.S.- Morocco FTA, Art. 15.11(28)(xi).)

For countries considering adopting an administrative subpoena, following is a discussion of some of the privacy and due process concerns raised by the U.S. expedited subpoena.

1. **U.S. copyright holders have used this provision to create an automated disclosure regime for ISPs that bypasses established judicial review standards. This process has significantly increased ISPs' potential liability and jeopardized Internet users' privacy**.

Unlike the existing subpoena process in U.S. law that required a judge to balance the subpoena target's rights with the evidence and need for the information sought, the DMCA subpoena process has no provision for judicial oversight and has substantial procedural due process deficiencies. First, since ISPs have no legal obligation to notify a customer that his or her identity has been sought, an Internet user may not learn of the subpoena. Even where a subscriber is notified of the subpoena, he or she is not afforded any formal right to be heard and to have a judge evaluate a claim of mistaken identification, through a legal representative, before the ISP discloses his or her identity. In cases where there has been a mistaken identification,[20] the subscriber has no statutory right of action or recourse against a mistaken copyright owner or the ISP.

2. **The expedited subpoena power carries a significant potential for misuse and may be inconsistent with the existing discovery procedures under U.S. trading partners' national law, which often requires judicial approval before subpoenas are issued**

In order to obtain a subpoena from a court clerk under section 512(h), a person need only *claim* that his or her copyright has been infringed. And, unlike existing pre-lawsuit discovery procedures in U.S. law, the DMCA subpoena procedure does not require a copyright owner to actually file a copyright infringement lawsuit upon obtaining a subscriber's identity. Therefore, an unscrupulous copyright owner or purported copyright owner could use the subpoena process to obtain subscribers' identities with no intent of ultimately filing suit.

---

noted, even though copyright owners use "bots" to send out notices with no due diligence, each notice requires human intervention by the ISP to see if they are valid or not.

[20] *See Unsafe Harbors: Abusive DMCA Subpoenas and Takedown demands*, Electronic Frontier Foundation report, available at <http://www.eff.org/IP/P2P/20030926_unsafe_harbors.php>

The lack of judicial oversight also facilitates the automation of the subpoena issuance process. In the U.S., music copyright holders issued over 3000 subpoenas to ISPs across the United States from July to December 2003, resulting in thousands of individual lawsuits against individual subscribers. The U.S. subpoenas required ISPs to provide the requested information within 7 days, compliance with which has imposed a substantial resources and cost burden on ISPs. Adopting a DMCA-style automated subpoena process, which facilitates a high volume of subpoenas and short response period, is likely to increase ISPs' potential exposure to liability due to errors in disclosure of subscriber identification. In the U.S. there have been at least three reported instances where the wrong person was identified in the subpoena process, and in two cases, subsequently sued.

The expedited subpoena process has raised much controversy within the United States, but at the same time has proved to be unnecessary for U.S. rightsholders to enforce their rights against alleged file-traders. Since December 2003, U.S. rightsholders have ceased using the expedited subpoena process to identify alleged file-sharers following two court rulings that found it did not apply to situations where allegedly infringing works were stored on users' own computers.[21] Instead, a total of over 10,000 U.S. lawsuits have been filed against individual alleged file-traders, the majority of which have been "John Doe" anonymous lawsuits, using existing procedures in U.S. law that predate the DMCA.

3. Increased operating costs for ISPs

The use of expedited subpoenas and court-ordered subpoenas in the "John Doe" lawsuits filed by the Recording Industry of America, has increased the operating costs of U.S. ISPs. Any country considering implementation of these provisions should bear in mind the economic impact of the thousands of expedited DMCA subpoenas issued to U.S. ISPs between July and December 2003, the lawsuits over subpoena compliance between the R.I.A.A. and ISPs Verizon Communications, Inc., SBC, Cox Communications, and Charter Communications, Inc. respectively, and the subpoenas issued to U.S. ISPs in the thousands of "John Doe" lawsuits by Recording Labels against individuals identified only by IP address[22]. For instance, ISP Charter Communications, Inc., has stated that the annual cost of complying with R.I.A.A. subpoenas is likely to run to several hundred thousand dollars[23].

Gwen Hinze
International Affairs Director
Electronic Frontier Foundation

June 7, 2005

---

[21] *Recording Industry Association of America v. Verizon Internet Services, Inc*. (D.C. Court of Appeals, Case No. CV 02-MS-0323, Consolidated with No. 03-7015, 19 December 2003); *Pacific Bell Internet Services v. R.I.A.A. et al* (N.D.Ca., C 03-3560, filed 30 July 2003); *R.I.A.A. v. Charter Communications*, (8th Circ., No. 03-3802, January 4, 2004), all available at http://www.eff.org/IP/P2P/riaa-v-thepeople.php.

[22] For a selection of these lawsuits, see EFF's website, http://www.eff.org/IP/P2P/riaa-v-thepeople.php.

[23] See Charter Communications, Inc.'s Motion to Quash Subpoena Served by the Recording Industry Association of America, E.D.Mo., Case No. 4:03MC00273CEJ, October 3, 2003, paragraph 6, at <http://www.eff.org/IP/P2P/20031003_motion_to_quash.pdf>.

SELECTED FURTHER RESOURCES:

Internet Intermediaries in General:

Dr. Charlotte Waelde and Lillian Edwards*, Online Intermediaries and Liability for Copyright Infringement,* prepared for World Intellectual Property Organization seminar on Copyright and Internet Intermediaries, April 18, 2005, available at: http://www.wipo.int/meetings/2005/wipo_iis/en/presentations/doc/wipo_iis_05_ledwards_cwaelde.doc

U.S. Provisions:

Unsafe Harbors: Abusive DMCA Subpoenas and Takedown Demands, Electronic Frontier Foundation report, available at:http://www.eff.org/IP/P2P/20030926_unsafe_harbors.php\

Digital Millennium Copyright Act of 1998, U.S. Copyright Office Summary, available at: http://www.copyright.gov/legislation/dmca.pdf

Jonathan Band and Jenny Marcinko, *A New Perspective on Temporary Copies: The Fourth Circuit's Opinion in Costar v. Loopnet*, 2005 STAN. TECH. L. REV.P1, available at http://stlr.stanford.edu/STLR/Events

David Hayes, *Advanced Copyright Law on the Internet*, (February 2004), available at: http://www.fenwick.com/docstore/355/Advanced_Copyright_02-29-04.pdf

(Previous versions published in The Computer Law & Security Report, Part 1, November/December 2000, at 363, Part 2, January/February 2001, at 3, Part 3, March/April 2001, at 75, Part 4, May/June 2001, at 147, Part 5, July/August 2001 at 219, Part 6, September/October 2001 at 291, Part 7, November/December 2001 at 363, Part 8, January/February 2002 at 3; and 7 Tex. Intell. Prop. L. J. 1 (Fall 1998))

Professor Jessica Litman, *DIGITAL COPYRIGHT*, Prometheus, 2001.

David Nimmer, *Repeat Infringers*, 52 JOURNAL OF THE COPYRIGHT SOCIETY OF THE U.S.A. 170 (WINTER 2005).