# THE LITIGATION NEWSLETTER

WINTER 2008

## WHAT'S INSIDE:

Address correspondence and items for publication (hard copy and disk if possible) to:

**Dari Craven Bargy** *Esq.*
**MILLER CANFIELD PADDOCK & STONE**
**444 West Michigan Avenue**
**Kalamazoo, Michigan 49007**
**(269) 381-7030**
**Email: bargy@millercanfield.com**



# CHAIR'S LETTER

**by:** ***Susan Wilson Keener***

*Keener Law Offices, PLC*

Dear Colleagues:

The Litigation Winter 2008 newsletter is my first opportunity to address the entire Litigation Section, although my term as chair started in October, 2007. I hope you took note of the "new look" for the newsletter. Credit for our fresh New Year look goes to the newest newsletter editors, Dari Craven Bargy and Lynn Shecter. They have diligently taken on their new roles in bringing a more user-friendly and exciting format to the newsletter with more new ideas to follow.

The theme of this issue is "Litigation In Cyberspace." Thinking about the articles in this newsletter and reflecting on my 23 plus years of practice as a litigation attorney, I pondered how the development of the Internet and information technology have had such an amazing impact on our world and daily life and concluded that these developments have had no less impact on litigation and the daily practice of law. When I began practicing in the mid 1980's, I did not have a PC on my desk or laptop in my briefcase. I did not surf the net. Today, I cannot survive without my laptop. When I have technology "issues" at work, I find that my office is nearly paralyzed. The importance of the Internet and use of information technology has now permeated all aspects of the law and is more and more an issue in litigation. Therefore, our newsletter team concluded that focusing on litigation in cyberspace would be an appropriate theme for our first newsletter of 2008.

I wish to thank the Information Technology Law Section (formerly known as the Computer Law Section) for contributing the articles in this newsletter. We as litigators often turn to other experts or educate ourselves on substantive areas of law when faced with a new issue to litigate. The Information Technology Law Section provides that expertise to us in this issue. For your information, the Section focuses on developments in the law relating to information technology, including intellectual property, software licensing, e-business, internet, e-crime and litigation issues. Its membership is diverse, as members span all disciplines and practices. If you would like to know more about this section or to join the Information Technology Law Section, contact the chairperson Kimberly Paulson at paulson@millercanfield.com.

Next, I must thank our immediate past chair of the Litigation Section, Brad Sysol, whose excellent leadership eased my transition to assuming the role of chair, but left me with very large shoes to fill. Brad led the Section well, serving as the editor of last year's newsletters, in addition to fulfilling his role as chair. Brad's leadership was instrumental in achieving the highest ever number of attendees at our summer conference in 2007. Brad has also worked hard to find strong leaders within the Council to support me in serving as the other officers of the Section. I am looking forward to a productive and exciting year with James Partridge, Bonnie Sawusch, and Tom Cavalier as we steer the Council through the remainder of my term.

The Council will continue its partnership with the Institute of Continuing Legal Education and Shel Stark in bringing exciting educational programming to the members of the Section and the Bar in general. We will continue our Masters in Litigation and Litigation Boot Camp Series and our outstanding summer conference event. In addition, the Council plans to spend some time at each business meeting discussing issues of importance and interest to the practice of litigation. We want to make sure that the Council is diligent in keeping the Section informed of pending legislation and court rule changes that will affect our practice. Our section is also fortunate to have a healthy operating fund, and we are exploring ways this year to invest some of the budget surplus in new projects to benefit our membership and section.

We are always looking for members of the Section who might be interested in serving on the Council and continue to seek ways to enhance our representation of this diverse section of the State Bar of Michigan. We seek geographic representation from around the state, persons who work in various fields of litigation practice and in forms of practice (such as solo, firm or corporate), in addition to more traditional forms of diversity. In essence, we are looking for a few good litigators who would be interested in working with us during an exciting time for the Section. If this kind of exciting bar activity interests you, feel free to contact me about openings on the council or committees where your talents can be used.

A great way to learn more about the Council is to attend our summer conference, where you can enjoy networking in a family-friendly atmosphere while brushing up on your litigation skills with superior continuing legal education. Last year, conference attendees raved about the mountain top reception where Council and section members networked with family members feeling equally entertained and enjoying all that Northern Michigan has to offer. We will be repeating this popular event. We are also fortunate enough to have as our speaker Gerry Williams, a nationally known speaker who presents excellent "hands on" negotiation seminars. He will present "The Complete Legal Negotiator". You will not want to miss this wonderful program, so save the date on your calendars now and read more about the event in this and upcoming notices. On behalf of the officers and Council of the Section, we welcome your input and participation in our section's activities and continuing legal education offered in the upcoming year by the Section.

Sincerely,

Sue Keener

**IMPORTANT DATES**

| | |
|---|---|
| *January 10, 2008* | Litigation Section Meeting at 5:30 p.m. via telephone conference* |
| *March 12, 2008* | Litigation Section Meeting at 5:30 p.m., Lansing |
| *May 14, 2008* | Litigation Section Meeting at 5:30 p.m. via telephone conference |
| *July 25-26, 2008* | Summer Conference at Shanty Creek Resorts, Bellaire, Michigan |
| *September 2008* | Litigation Section Meeting at State Bar Annual Meeting |

**Meetings are open to all members. Please contact Susan Wilson Keener at skeener@keener-law.com*

# LITIGATING AN ONLINE CASE: The Real World Challenges

by: *Kimberly A. Paulson**

More and more transactions now take place online. No doubt about it, the Internet is here to stay. As a result, more lawsuits arise from activities undertaken online. If you have not already, you will eventually be called to represent a client in an "online case" – one that has arisen based on online activities. Regardless of your level of litigation experience, the online case can make you feel like a novice, as it presents unusual and often challenging issues not encountered in traditional litigation. Understanding and anticipating the unique issues that you may confront is an important first step to dealing with them handily when they arise. This article addresses some of the most common challenges you are likely to face.

## WORLDWIDE SCOPE

The Internet has made the world smaller. Residents from different parts of the globe can easily come together to chat, play games, or engage in commercial transactions. Of course, this is one of the wonderful features of the Internet, but it can create a nightmare for litigators. Suddenly, the issues of where to sue, what law applies and whether a party is even amenable to process loom large. Just determining where the relevant parties and witnesses reside can be very difficult. If you are lucky enough to figure it out, you still need to determine whether they are amenable to process in the United States and if they are even bound by U.S. law. Answering the question of "where" the offending conduct took place is also difficult, as the Internet has no geographic boundaries.

Determining proper jurisdiction, for instance, can be challenging. The *Zippo*[1] test is still useful when the defendant is the operator of a website or online operation, but it does not cover all situations. For instance, if you are litigating against an individual user using a third-party site, the question is a more complicated one. Generally courts try to apply traditional long arm statutes and jurisdictional principles to the unique circumstances of the Internet with varying results.

Contrary results have been reached with respect to online auctions. In *Sayeedi v. Walser* the court found that it did not have jurisdiction over an out-of-state defendant who sold goods into the state via a single eBay auction. 835 N.Y.S.2d 840 (N.Y. Civ. Ct. 2007). In contrast, the U.S. District Court for the Eastern District of Michigan reached the contrary result where the seller was a sophisticated commercial merchant advertising extensively and engaging in regular and systematic use of eBay to sell its goods. *Dedvukaj v. Malone*, 447 F.Supp.2d 813 (E.D. Mich. 2006). The cases applying long arm statutes demonstrate that a litigator must be aware of the full extent of the parties' online activities, whether they were directed at a particular jurisdiction, and where the effects of the conduct were felt in order to effectively evaluate whether jurisdiction can properly be exercised in an online case. Sometimes, though, these facts are difficult to discern because of the nature of online activity. Previous cases may provide guidance as to what factors will be found to be relevant and which will not.

The worldwide scope of the Internet also complicates determining which jurisdiction's law applies. Choice of law can, under ordinary circumstances, be a tricky issue. The issue is made even more difficult in Cyberspace. A litigator should never discount or overlook the role that Internet activity can play in such a determination. Courts, for instance, often find the location of a server at issue persuasive. In *Wiest v. E-Fense, Inc.*, an online defamation case, the court found that because "'the website in question is controlled from Defendant E-Fense, Inc.'s corporate headquarters located in Virginia,' and the allegedly defamatory statements were published on this website, Virginia law applies." 356 F. Supp.2d 604, 608 (E.D. Vir. 2005). In *American Online v. Nat'l Healthcare Discount*, AOL sued an Iowa corporation that allegedly hired e-mailers to send unauthorized and unsolicited bulk e-mail advertisements to ISP's customers, thereby burdening AOL's servers and causing AOL harm. The court found that because AOL's allegedly overburdened server was located in Virginia, thus resulting in economic harm in that state, Virginia was the site of injury and its law applied to the action. 121 F. Supp.2d 1255, 1270 (N.D. Iowa 2000).

*Ms. Paulson is an attorney at Miller, Canfield, Paddock and Stone, where she practices commercial litigation, with an emphasis on IP and IT issues. She is also the current Chairperson of the Information Technology Law Section of the State Bar of Michigan. She can be contacted at paulson@millercanfield.com.

However, it is important to keep in mind that when the primary conduct at issue occurs off-line, related online activity may not hold much weight. In *Carris v. Marriott Int'l, Inc.*, the court held that U.S. law did not apply to a personal injury suit between an Illinois resident and a Bahamian hotel despite the fact that the plaintiff made his hotel reservations via an internationally accessible web site. 466 F.3d 558 (7th Cir. 2006). Importantly, *Carris* demonstrates that even if a website is interactive enough under *Zippo* to make jurisdiction proper in the U.S., it may not necessarily be enough to justify application of U.S. law.

## ANONYMITY

It is relatively easy to remain anonymous in Cyberspace. While that feature of the Internet is great for freedom of expression, it can create serious problems for litigation. Trying to determine the true identity of a defendant can be very difficult, or in some cases even impossible. If the Internet user has registered through an ISP or website, sometimes the user's identity can be obtained from that source, using the user's pseudonym or IP address. Litigators should search relevant websites to determine what the particular online provider will require in order to turn over user information. Often, the online provider will require that you serve it with a subpoena or court order before it will turn over information, which will, obviously, require the filing of a lawsuit or some form of court action before a user's information can be obtained. Often this is done through a John Doe suit. Also, some statutes authorize information seeking subpoenas in particular situations. For instance, the Digital Millenium Copyright Act ("DMCA") authorizes issuance of subpoenas by a copyright owner for the purpose of identifying an alleged online infringer. 17 U.S.C. § 512 (h).

Not surprisingly, many online providers will still object and move to quash, as they risk losing users if they are perceived as giving out user information too easily. Courts in different jurisdictions apply different tests with respect to whether to enforce such subpoenas, and the level of scrutiny applied varies depending upon the extent to which the users' First Amendment rights are affected. *See, e.g., Best Western Int'l v. Doe*, No. CV-06-1537-PHX-DGC, 2006 WL 2091695, *4 (D. Ariz. 2006)(applying summary judgment standard where First Amendment interests were strong); *Immunomedics, Inc. v. Doe*, 775 A.2d 773, 776-77 (N.J. Super. Ct. 2001) (applying balancing test). Do your research ahead of time to determine what standard you will need to meet if your subpoena is challenged.

Keep in mind though, that even if the online provider complies with your information request, the information revealed may not be helpful. In many cases, online providers simply do not require users to provide much information and often do not verify the information they receive. This is especially true if registration or use of the site is free. Moreover, a savvy user can find ways to remain anonymous if she truly wants to.

## SAFE HARBORS

The Digital Millenium Copyright Act ("DMCA") and the Communications Decency Act ("CDA") both contain safe harbor provisions that grant limited immunity solely to online providers. The Anticybersquatting Consumer Protection Act ("ACPA") also provides for limited immunity with respect to domain name administrators. If you are seeking to sue an online provider or domain name administrator, before you go to the time and effort of commencing a lawsuit you should review these safe harbors, in light of the facts of your case, to determine whether you can even establish liability. On the flip side, if you are defending an online provider or domain name administrator, you need to be prepared to argue in favor of safe harbor for your client.

The DMCA's safe harbor scheme is somewhat complicated. It provides immunity for four separate functions performed by online providers, and then only if the provider has complied with certain conditions. 17 U.S.C. § 512 (a-d). It also limits the liability of non-profit education institutions. 17 U.S.C. § 512 (e). Further, it provides immunity for the good faith "take down" of infringing material. 17 U.S.C. § 512 (g). The definitions, conditions and requirements are extensive. However, it is worth the effort of wading through the text, because the immunity provided can be very valuable to a service provider and detrimental to a plaintiff in an infringement case.

The safe harbor provided by the CDA is more straightforward. It provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230 (c)(1). It also provides that such a provider cannot be held liable for actions "taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable." 47 U.S.C. § 230 (c)(2)(A). It also shields the provider from liability for providing information content providers with the means to restrict access to such material. 47 U.S.C. § 230 (c)(2)(B).

The ACPA's safe harbor is probably the simplest of the three. It limits the liability of a domain name registrar

only to situations involving bad faith or reckless disregard. 15 U.S.C. § 1125 (2)(D)(ii). This protects a domain name registrar from becoming embroiled in and being held liable in a basic domain name dispute in which it has essentially done nothing wrong.

These safe harbors are routinely invoked and enforced by courts. Don't forget them when litigating an online case.

## UNDEVELOPED LAW

When litigating an online case, even one of the simplest determinations, identifying the causes of action becomes challenging. Frequently, new online legal questions arise that the law has not yet addressed. Legislatures are slow to respond, so courts are left to formulate creative new applications of existing laws.

In recent years, for instance, the traditional tort of trespass has been adapted to apply to some online situations. *See, e.g., Sotelo v. Direct Revenue*, 384 F. Supp.2d 1219 (N.D. Ill. 2005)(holding that spyware may constitute trespass to personal property); *eBay, Inc. v. Bidders Edge*, 100 F. Supp.2d 1058 (N.D. Cal. 2000)(holding that using bots to conduct unauthorized "crawling" of servers may constitute trespass to chattels). The same is true of the tort of conversion. *See, e.g., Kremen v. Cohen*, 337 F.3d 1024 (9th Cir. 2003) (improperly transferring ownership of domain name may constitute conversion). All the contours of the application of these types of claims to online activity have yet to be seen, though. That means that case law provides some guidance, but probably not enough. A litigator handling an online case still needs to think creatively, relying not only upon traditional online claims but those that normally apply only off-line. Courts seem willing to at least consider applying off-line causes of action to online activity as long as the claim is feasible.

## ONLINE CONTRACTS

It is best for a lawyer handling an online case to do her own preliminary research to determine whether her client might have agreed to certain terms before commencing suit. Often these contracts present themselves as "terms of use" on a website or a license agreement for the downloading of software and may consist of a "click-wrap" or "browse-wrap" agreement. Importantly, these agreements often address litigation issues such as jurisdiction, choice of law, warranties and remedies available, and sometimes include arbitration clauses. Of course, lawyers deal with these provisions in "real world" contracts all the time, but there are several differences when dealing with online contracts.

First, as opposed to contracts made off-line, Internet users are often less likely to realize or remember they have entered into an online contract. Clicking an "I agree" box has become so routine to Internet users, that many do not even give it a second thought. Second, even if users realize they have entered into an agreement, they are probably less likely to have read the terms of said contract. Third, it is also less likely that an Internet user has kept a copy of the online contract. The end result is that a lawyer representing that user is unlikely to even realize that a contract exists. That is why it is highly advisable for a lawyer to determine whether her client has likely agreed to certain terms, by reviewing the website or online transaction herself. In addition, because online providers often amend their online agreements, a lawyer must try to determine which version her client agreed to.

Once you have determined that an online contract exists, and its terms, you need to examine its enforceability. While online contracts are generally enforceable, and are subject to the same general defenses as their off-line counterparts, there are some unique issues that will affect the enforceability of online contracts. Because of the nature of online contracts, courts have looked to aspects such as how the contract was presented, how big the text was, how long the contract was, whether important language was hidden in the middle of imposing text, and whether the user had to affirmatively assent to the contract.

For instance, in *Defontes v. Dell Computers Corp.*, the court found that the arbitration agreement contained in an online browse-wrap agreement was not enforceable because the terms of the agreement could only be viewed via a hyperlink inconspicuously located at the bottom of the web page. No. C.A. PC 03-2636, 2004 WL 253560 at *6 (R.I. Super. Ct. Jan. 29, 2004). The court held that was "not sufficient to put Plaintiffs on notice of the terms and conditions of the sale of the computer." *Id.* Similarly, in *Specht v. Netscape Communications*, the court also found an online agreement unenforceable when the circumstances surrounding assent to the agreement did not make it clear to the user that he was entering into an agreement. 306 F.3d 17 (2d Cir. 2002).

## CONCLUSION

As the law adapts to the Internet Age, so must litigators. Online cases present a myriad of challenges not usually encountered in traditional cases, but familiarizing yourself with these unique issues will allow you to anticipate them. Being creative and flexible and doing

your homework ahead of time will allow you to navigate an online case (relatively) unscathed.

**ENDNOTE**

1. In *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, the court set forth a sliding scale test with respect to the level of interactivity of a party's web site for purposes of determining whether that party can properly be subject to specific personal jurisdiction. 952 F.Supp. 1119 (W.D. Penn. 1997). Under this test, the more interactive the party's site, the more likely the party can be properly subject to specific personal jurisdiction. *Id.*

# COUNTERFEIT SOFTWARE: AN OVERVIEW OF "WILLFUL BLINDNESS" AND BEST PRACTICES

by: *Kathryn L. Ossian & Carla M. Perrotta*

## OPEN YOUR EYES: NO SUCH THING AS LEGALLY BLIND

When it comes to licensing software, your clients or even your firm may try to cut costs by finding the distributor with the lowest price. Care must be taken, however, to make sure that the software is authentic and not counterfeit.

A recent decision by the U.S. Court of Appeals for the 7th Circuit reinforces this point. *Microsoft Corporation v Aleks Rechanik* No. 06-4343 (7th Cir. 2007) (found at: http://www.altlaw.org/v1/cases/192877). Aleks Rechanik, an individual in the business of selling low cost software was sued by Microsoft Corporation for federal copyright and trademark infringement. 17 U.S.C. § 501; 15 U.S.C. § 1114(1). Microsoft alleged that the Microsoft programs being purchased and then sold by Rechanik's company were counterfeit. Rechanik admitted in his deposition that: (i) he did not purchase the products from authorized distributors, (ii) he did not ask whether the products were legitimate and (iii) he did not examine the software to determine whether it was authentic.

Rechanik argued that he did not know that the software was counterfeit and that, therefore, he should not be personally liable for the infringement. The court relied on *In re: Aimster Copyright Litig.*, 334 F.3d 643, 650, 655 (7th Cir. 2003) and rejected Rechanisk's argument, holding that his "ostrich-like business practices amount to willful blindness" that demonstrated the intent necessary to be a contributory infringer. The court therefore upheld a judgment of $880,000 against Rechanik in Microsoft's favor. *In re: Aimster* explains the notion that in copyright law (and the law in general), willful blindness is knowledge when the defendant should have known of direct infringement. *Id.* at 650.

## BEST PRACTICES

All businesses should keep track of exactly which software licenses they have and how many they are permitted to use. Below are some tips that you and your clients' companies may use to ensure compliance with software licensing terms:

1. DUE DILIGENCE. In *Microsoft v Rechanik*, the defendant admitted that he failed to take any measures to verify the authenticity of the software. When companies make software purchases, they should ensure that they are taking proper steps to determine authenticity. First, they should make sure the price is right. If the price seems too good to be true, it probably is. Companies should ensure their sources are legitimate, such as purchasing directly from an authorized dealer. Organizations should understand exactly what they are buying. Furthermore, companies should check that the software is properly packaged and labeled. If there are any doubts as to the legitimacy of the software, companies should speak directly with the software publisher. Moreover, if one person is the designated agent in an organization to purchase software licenses, the company should have appropriate checks and balances established to oversee that person's decision. Asking the right questions before purchasing the software may prevent confusion about what was purchased down the line.

2. COPYRIGHT AWARENESS. Sometimes employees need a friendly reminder that software programs are protected under the United States Copyright Act. 17 U.S.C. Illegal copying of software, whether intentional or unintentional, may result in fines or even imprisonment. In most cases involving company software piracy, large fines have been imposed due to the actions of only a handful of employees. For example, a 10-person architecture firm was the subject of a $67,000 demand from the Business Software Alliance (BSA), a software piracy watchdog group. Some of the firm's employees had downloaded unlicensed copies of software on company computers. http://www.examiner.com/a-1067334~Small_business_in_cross_hairs_of_software_piracy_crackdown.html. Clients should also be aware that this year, BSA began offering

*Kathryn L. Ossian is a principal and Information Technology Team Leader at Miller Canfield Paddock and Stone, P.L.C. She specializes in information technology law and is a member of the Computer Law Section of the State Bar of Michigan. Carla M. Perrotta is an associate attorney at Miller Canfield Paddock and Stone, P.L.C. She specializes in information technology law and is a member of the Computer Law Section of the State Bar of Michigan.*

$1 million rewards to disgruntled employees who anonymously report their employers' unauthorized software use. *Id.*

3. BE PROACTIVE, NOT REACTIVE. Companies shouldn't wait until the non-compliance is brought to light from someone within the company or, worse yet, the software vendor or a policing agency acting on the vendor's behalf. Organizations should conduct regular self-audits of the software programs that it licenses. Self-audits should be conducted at least annually to determine the actual number of licenses being used on the company's system(s). There are even several software programs available to help companies conduct efficient self-audits and keep track of their licenses. If the audit reveals an under-usage, any unused licenses should be reallocated. If the audit reveals an over-usage, check the licensing agreement for your obligations and any notification requirements. Companies should respond to an appropriate audit request from the software vendor.

In short, ensuring compliance with software licenses may be a bit of a hassle in the short run, but it can save time, money and possibly even your client's reputation, in the long run. By advising your client to take steps to establish and maintain true compliance, you may help your clients avoid the fiasco and possible embarrassment of software piracy.

# *SAVE THE DATE*

**Join your Litigation Section colleagues for the Program of the Summer!**

**WHAT:** 2008 Litigation Section Summer Conference
"The Complete Legal Negotiator" with Gerald R. Williams

**WHEN:** July 25-26, 2008

**WHERE:** The newly renovated Summit Village, Shanty Creek Resorts

**WHO:** Gerry Williams is Professor of Law, J. Reuben Clark Law School, Brigham Young University, Provo, Utah. More than 1100 practicing lawyers around the world have experienced the power of this leading pioneer researcher and teacher of real-world negotiation practice. Over and over, registrants have loved Gerry Williams, rating his program the best CLE they have ever attended!

Watch video presentations of spontaneous, unscripted negotiations, engage in voluntary exercises and learn strategies based on careful research to kick your skills up to the next level. Deal with persistently combative opponents like never before! "Good enough" is NOT good enough! Become the negotiator you have the potential to be. Gerry Williams promises a CLE experience on which you can build all the rest of your professional life! **For more information, call ICLE toll free at 877-229-4350.**

**WHY:** Lawyers today rarely try law suits; instead they negotiate them. Even the most experienced trial lawyers settle more cases than they take to trial. In this age where the American trial is vanishing, the practice of law has changed: Negotiated outcomes are the most obvious measure of your value to your clients! This intense, hands-on skill-building work shop is your opportunity to learn from the best, kick your skills up to the next level and improve results for clients! Bring your family to the newly renovated Summit Village hideaway for fun, entertainment and learning. Shanty Creek invested $10 million to make the Summit a premier destination! Join us and see. This will be the best program of the summer. Don't miss it!

# ENFORCING RIGHTS AGAINST ONLINE INFRINGERS: BRANDISHING THE DOUBLE-EDGED SWORD OF THE DMCA

**by:** ***Carol Ruth Shepherd****

*Attorney, Arborlaw PLC, Ann Arbor, MI*

The Digital Millenium Copyright Act (DMCA)[1] of 1998 was enacted to bring copyright enforcement more in line with the realities of digital technology and the Internet, where it is easier and speedier for millions of daily users to reuse content by cutting and pasting, than it is for them to create and publish original content. With the rise of content-sharing sites such as YouTube.com, the republication of copyrighted content has become so pervasive that litigation over the use of third-party content has become an ordinary news topic.[2] In seeking to use the DMCA's "takedown" procedure to enforce intellectual property rights, every rights owner is not only a potential plaintiff, but also a potential defendant – an unsophisticated rights owner can unwittingly expose itself to liability under the DMCA for false accusations of infringement. This article highlights the most common mistakes rights owners make in using the DMCA takedown procedure as a means of policing the unauthorized use of intellectual property.

## THE SECTION 512 TAKEDOWN PROCEDURE

In recognition of the significant costs and delay associated with federal copyright litigation, the DMCA added a "self-help" remedy to the Copyright Act. Section 512(c)(3)[3] allows copyright owners to achieve removal of allegedly infringing materials without filing suit, by contacting the online service provider and following a set of notice-and-information procedures set out in the statute. (The Section 512(c)(3) procedure is commonly referred to as a "takedown"). The procedure operates as follows: (1) a copyright owner swearing to a "good faith" belief of copyright infringement sends a notice conforming to the statutory requirements[4] to an online service provider, identifying contributed materials on the service which allegedly infringe the owner's rights; (2) the service provider removes the materials from the service as required under the statute to receive immunity from liability;[5] (3) the service provider notifies the contributor if a takedown occurs[6] and allows the contributor to make a counter-notice[7] rebutting the infringement allegation; (4) if the complainant turns out to be facially meritorious and the complaining copyright owner does not file suit within fourteen (14) days, the service provider must restore the materials.[8] The takedown procedure is wholly extrajudicial. Parties may (and do) seek judicial review for actions taken under Section 512(c)(3) which deviate from the statutory requirements.

The DMCA takedown procedure is well-known on the Internet and is wildly popular with large and small rights owners, and with third-party content contributors. Large Internet access providers and search engine sites are estimated to receive DMCA takedown notices numbering in the tens of thousands per year.[9] However – because it allows rights holders to achieve the removal of published materials without judicial oversight on a mere assertion of rights and an allegation of infringement – critics contend that the procedure is too widely abused, has a chilling effect on free speech and violates due process.[10] There is no doubt that the Section 512 takedown procedure has been widely used in inappropriate ways. Both individuals and large corporations routinely use the procedure aggressively, sending cease-and-desist letters to censor opinion, to suppress the online publication of unflattering or damaging content, to attack enemies and competitors, and to enforce non-copyright intellectual property claims. Several companies and performing rights organizations use automated "robots" to search for infringing content and subsequently file erroneous takedown letters identifying the wrong party or completely unrelated materials.[11] A 2005 survey found that over a third of takedown requests were not appropriate under the statute.[12]

## SECTION 512 TAKEDOWN TRAPS: INTERNET FORM LETTERS AND WEB COMPLAINTS

Businesses that routinely threaten civil litigation in the course of hashing out disputes over their

**Carol Shepherd is in private practice in Ann Arbor concentrating in information technology transactions and business law. She is a past chairperson and council member of the Information Technology Law Section and a past council member of the Arts, Communication, Entertainment and Sports Law Section.*

commercial transactions are in for a rude surprise under the Copyright Act. Section 512(f)[13] explicitly provides a remedy for "bad faith" takedown notices and misrepresentations about copyright infringement, holding that a party may be ordered to pay the aggrieved party's damages, costs and attorneys' fees for making "knowing" and "material" misrepresentations under Section 512.[14]

Rights holders, typically acting without an attorney in choosing to make their own DMCA takedown demands, can get "trapped" in Section 512(f) suits or counterclaims in two common ways: (1) they use an inappropriate form letter which fails to comply with the requirements of the statute and/or makes inappropriate non-copyright legal claims under the takedown framework; or (2) they rely on a service provider's procedure for notice and takedown of materials, which may steer them unwittingly into making fraudulent claims under Section 512(f).

A rights owner using the Section 512 takedown procedure will typically give notice via a takedown email or letter. Most Section 512 notices are sent electronically as e-mail[15] (although many are sent by surface mail or fax to the service provider if no e-mail address for legal notices is readily apparent or available). Because Section 512 is well-known to rights holders to be a "self-help" procedure that results in the speedy and automatic removal of the undesirable materials 90%+ of the time, the vast majority of complaining rights owners fashion their own demands by merely cutting and pasting seemingly-applicable text from publicly available letters. Thousands of actual and sample DMCA takedown letters are posted on the Internet.[16] Many of these notices defectively allege copyright infringement under the Section 512(c) protocols and are entitled to be disregarded by the service provider's DMCA agent. Others threaten suit under the aegis of the DMCA for causes of action sounding in trademark, trade secret, privacy or publicity. Still others complain about publication or use which is clearly permitted under copyright law (such as "fair use" of copyrighted material,[17] resale of copyrighted materials under the "first sale" doctrine,[18] or the publication of public-domain content or content expressly available for use without restriction under a Creative Commons or open-source GPL license[19]).[20] For erring rights holders, a suit for damages under Section 512(f) can have severe consequences: the rights owner in one leading case settled in the face of a Section 512(f) counterclaim for damages in an agreed amount of $125,000.[21]

A second DMCA trap for the unwary rights owner is the service provider's own web-based complaint form. Online service providers frequently fashion their own notice-and-takedown procedure for reporting intellectual property violations as a means of creating an efficient internal workflow to deal with the hundreds of notices they receive. Many of these provided notice forms conflate various intellectual property issues, including legitimate DMCA claims as well as illegitimate ones – but may nevertheless track the protocol and remedies under DMCA Section 512, leading an unsophisticated rights owner to believe that the DMCA takedown remedy is available for non-copyright grievances.

For example, ebay.com provides rights owners with a VeRO (Verified Rights Owner) complaint form that allows a complainant to allege that an item for sale "is an unlawful copy of media (software, games, movies, etc.)" under a copyright violation category called "Item Infringement."[22] While this allegation would be legally appropriate against the sale of counterfeit and knockoff goods, rights owners frequently assert this against dealers and resellers, erroneously believing that they may restrict or prohibit the resale of copyrighted works on sites such as Ebay.com.[23] Ebay sellers whose items have been de-listed due to a VeRO takedown frequently threaten a lawsuit for Section 512(f) fraudulent misrepresentation of copyright infringement and demand settlement damages for lost sales.[24]

## LITIGATION AGAINST RIGHTS OWNERS FOR SECTION 512(F) VIOLATIONS

As of this writing, a handful of cases have seen decisions or resolution with regard to violations of Section 512(f), with the primary litigated issue being the proper standard for determining whether a rights claimant is making a "knowing misrepresentation." Two 512(f) cases have generated court rulings that say the "good faith" belief of infringement required for filing a Section 512 takedown notice is *objective*, following the general principle that "ignorance of the law is no excuse." *In Online Policy Group v. Diebold*[25] and *Marvel Enterprises v. NCSoft*,[26] both courts held that having a "good faith" belief of infringement as specifically required to be entitled to a takedown under Section 512(c), means that the rights owner filing a takedown notice has a responsibility to know whether an online publication is or is not actionable as an infringement under the Copyright Act. Under this test, failure to meet an objective standard of "good faith" satisfies the "knowing misrepresentation" requirement for a takedown request to constitute a violation of Section 512(f). The only federal appellate case providing guidance on Section 512(f), *Rossi v. Motion Picture Association of America*,[27] disagrees with *Diebold* and *NCSoft*, holding that the standard

for determining whether a complainant is "knowingly misrepresenting" a claim of copyright infringement under Section 512(c) is *subjective* to the "good faith" belief of the rights owner.

The *Diebold* case is notable not only for its DMCA implications, but also for the important public policy and free speech issues underlying the case. Diebold, a provider of electronic voting equipment, has been widely criticized for its electronic voting software. Several sources have claimed that the software is defective and can be easily hacked to manipulate election results. In the Diebold case, the targets of Diebold's Section 512 takedown request were college students from Swarthmore who had discovered Diebold employee emails referencing internal company issues with the software, and who had posted the Diebold emails online for purposes of discussing the software's flaws, and the election fraud implications.

The Electronic Frontier Foundation (EFF) brought a counterclaim against Diebold under Section 512(f), asserting that Diebold knowingly misrepresented its copyright rights. It seems undisputable that Diebold, as an employer, would own copyrights in the emails of its employees, under the "work for hire" doctrine of the Copyright Act,[28] entitling it to prevent republication of the emails. However, it is also undisputable that the importance of allowing the public to discuss the security and reliability of electronic voting methodology, and issues with specific voting software, make an extremely strong case for applying the "fair use" exceptions for "criticism, comment, news reporting, teaching, scholarship or research."[29] The court ruled against Diebold, noting that "the email archive was posted or hyperlinked to for the purpose of informing the public about the problems associated with Diebold's electronic voting machines. It is hard to imagine a subject the discussion of which could be more in the public interest. If Diebold's machines in fact do tabulate voters' preferences incorrectly, the very legitimacy of elections would be suspect."[30] The company did not appeal, but chose to settle the case (commentators have observed that the publicity backlash generated by fighting a "free speech" "voting rights" case with copyright technicalities probably motivated Diebold to cut its losses).[31]

In the *Rossi* case, the publisher operated an independent movie website. The Rossi site had a clickable link that read "Download movies here." The MPAA sent a Section 512(c) takedown notice to Rossi's hosting service provider, who immediately took down the site, costing Rossi lost profits in the form of lost advertising revenue. Rossi brought a Section 512(f) claim against the MPAA, arguing that the materials being complained of were not even on the Rossi site but on another site linked to from the Rossi site and that as a matter of law, linking to a website which may or may not contain infringing materials does not constitute copyright infringement. Rossi argued that the MPAA should have exercised reasonable due diligence before sending its Section 512(c) takedown notice – if the MPAA had only followed the links on his site, it would have discovered that the site containing the allegedly infringing materials was not part of Rossi's site or under his control. The federal district court held there was no requirement for a rights owner to conduct an investigation prior to filing a takedown notice to allege a "good faith" belief of infringement. Rossi appealed. The Ninth Circuit held that requiring a rights holder to conduct an investigation prior to filing a takedown notice would be to require a "reasonable and objective" standard in determining whether a takedown demand was made knowingly and in misrepresentation. The *Rossi* court noted that several other federal statutes traditionally held "good faith" to encompass a subjective standard and ruled that the "good faith" required by Section 512(c) is a subjective state of mind consisting of "honesty in belief or purpose," holding "a copyright owner cannot be liable simply because an unknowing mistake is made, even if the copyright owner acted unreasonably in making the mistake."

The subjective standard for "good faith" in making a Section 512(c) takedown request was further extended in *Dudnikov vs. MGA Entertainment*.[33] In the *Dudnikov* case, the Dudnikovs were eBay merchants who were selling BRATZ® dolls and merchandise on eBay. MGA, the owner of intellectual property rights in the BRATZ® characters and associated merchandise, filed an eBay VeRO takedown request against the Dudnikovs, resulting in the takedown of the auctions. The VeRO claimed copyright and trademark infringement and infringement of manufacturing, distribution, licensing and merchandising contract rights. The Dudnikovs were not authorized distributors or resellers of BRATZ® merchandise but claimed the "first sale" doctrine as a defense to copyright violations. They counterclaimed under Section 512(f), citing copyright misuse and damages from lost sales due to the disruption caused the VeRO takedown. MGA's motion for summary judgment on 512(f) claims was granted by the magistrate based on an affidavit of MGA's attorney that the viability of the claims were admittedly not investigated at the time the notice was filed. The Dudnikovs argued that MGA's attorney should be held to a higher professional standard and should have "known better" than to claim infringement because the offered items were subject

to the "first sale" doctrine. Following *Rossi*, the District Court upheld the magistrate's dismissal of the 512(f) issue on summary judgment, effectively stating that a sworn statement constituted a "good faith belief" as a matter of law.[34]

The pace of litigation under Section 512(f) for erroneous 512(c) takedown requests is steadily accelerating, with over ten cases currently in progress.[35] Intellectual property rights owners seeking to wield the sword of the DMCA Section 512 takedown to remove online content need to be wary of the weapon, and proceed carefully with the advice of counsel to avoid injuring themselves.

**ENDNOTES**

1. Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998). The Digital Millenium Copyright Act is available online at http://copyright.gov/legislation.dmca.pdf.

2. "Viacom Sues Google Over YouTube Video Clips," New York Times, March 13, 2007.

3. 17 U.S.C. § 512(c)(3).

4. Section 512(c)(3) sets out the elements for notification under the DMCA. Subsection A (17 U.S.C. 512(c)(3)(A)) states that a notification must include (1) a physical or electronic signature of a person authorized to act on behalf of the owner of the infringed right; (2) identification of the copyrighted works allegedly infringed; (3) identification of the material that is claimed to be infringing that is requested to be removed; (4) information reasonably sufficient to permit the service provider to contact the complainant; (5) a statement under penalty of perjury that the complainant has a "good faith" belief that use of the material is not authorized by the copyright owner; and (6) a statement that information in the notice is accurate and that the complainant is authorized to act on behalf of the copyright owner. Subsection B (17 U.S.C. 512(c)(3)(B)) states that if the complainant does not substantially comply with the statutory requirements, the notice will not serve as actual notice for the purpose of Section 512.

5. In return for cooperating with complainants, online service providers are shielded from liability for contributory copyright infringement, provided they comply with the following statutory requirements: (1) the service provider must be an entity offering the transmission, routing, or providing of connections for digital online communications (§512(k)(1)(A)); (2) the service provider must designate an agent for DMCA violations, register the agent with the Copyright Office, and provide a means through the service for rights owners to access the agent (§512(c)(2)); (3) the transmission, routing, provision of connections or storage by the service provider is carried out by an automatic technical process (§512(a)(2)); (4) the service provider must not be the party initiating the transmission of the material (§512(a)(1)); (5) the contributor and not the service provider, must select the origination and destination points of the contribution (§512(a)(3) and §512(k)(1)(A)); (6) the contribution must be transmitted "through" the system or network of the service provider (§512(a)(2)); (7) the service provider must not modify the contribution (§512(a)(5)); (8) no copy of the contribution may be maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients (§512(a)(4)); and (9) no copy of the contribution may be maintained on the system or network for a longer period than is reasonably necessary for the transmission, routing, and intended availability of the contribution (§512(a)(4)). An informal survey of websites, blogs, Internet access providers and many web hosting companies will reveal that the majority of online service providers are not registered with the Copyright Office and are not otherwise in compliance with the requirements of Section 512, legally exposing them to claims for contributory copyright infringement.

6. Online service providers are not required under §512 to notify the contributor that a takedown notice has been received, but are required to notify contributors if and when materials are removed. Large service providers typically remove material within one to three days of receiving a compliant notice.

7. 17 U.S.C §512(g)(3). A proper counter-notice under §512(g) must include (1) the user's name, address, phone number and physical or electronic signature; (2) identification of the material and its location before removal; (3) a statement under penalty of perjury that the material was removed by mistake or misidentification; and (4) consent to local federal court jurisdiction, or if overseas, to an appropriate judicial body.

8. See §512(g)(A), (B) and (C).

9. See J. Urban & L. Quilter, "Efficient Process or 'Chilling Effects'? Takedown Notices Under Section

512 of the Digital Millennium Copyright Act," Santa Clara Computer & High Technology Law Journal (March 2006).

10. See M. Pollack, "Rebalancing Section 512 To Protect Fair Users From Herds Of Mice-Trampling Elephants, Or A Little Due Process Is Not Such A Dangerous Thing," 22 Santa Clara Computer & High Tech. L.J. 547 (March 2006). The §512(c)(3) takedown procedure is an active target of public-interest organizations such as the Electronic Frontier Foundation and ChillingEffects.Org which focus on free speech, censorship, public domain and fair use concerns. These are actively working for repeal or reform of the §512 procedure. The EFF has been active in litigating against rights owners on behalf of content publishers and contributors for improper DMCA claims. See http://www.eff.org/issues/dmca.

11. See "RIAA apologizes for erroneous letters," CNET's News.com (May 13, 2003) at http://www.news.com/2100-1025-1001319.html.

12. Urban and Quilter, above.

13. 17 U.S.C. §512(f) reads as follows: (f) Misrepresentations.—Any person who knowingly materially misrepresents under this section— (1) that material or activity is infringing, or (2) that material or activity was removed or disabled by mistake or misidentification, shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.

14. The same prohibition against fraudulent misrepresentation of copyright infringment to a service provider, also applies to contributors or publishers who file a counter-notice which willfully and knowingly makes an allegation of meritorious defense where none exists.

15. Due to the informal nature of email, unsophisticated complainants are far more likely to send a casual demand to their service provider without bothering to read or refer to the statutory language. While many service providers make reference to §512 of the DMCA, few provide the actual language of the section, or a link to it.

16. For a representative sample of takedown letters, including letters which constitute copyright misuse or do not comply with the highly specific requirements of §512(c), see http://eff.org and http://chillingeffects.org. For an example of a blog written and edited by a non-attorney offering "stock" DMCA takedown letters for use by rights owners, see http://www.plagiarismtoday.com/stock-letters/.

17. 17 U.S.C. §107.

18. 17 U.S.C. §109.

19. See http://creativecommons.org/. Creative Commons provides standardized license terms with minimal reuse restrictions which may be adopted voluntarily by copyright authors to indicate acceptable uses of their work. The GPL (Gnu Public License) is a similar standardized license of "open-source" material which provides for free incorporation and reuse of copyrightable material as long as the user consents to similarly publish and license any works incorporating GPL materials under the same GPL license terms. See http://www.gnu.org/copyleft/gpl.html.

20. See "Unsafe Harbors: Abusive DMCA Subpoenas and Takedown Demands," an Electronic Frontier Foundation white paper dated September, 2003, available at http://www.eff.org/wp/unsafe-harbors-abusive-dmca-subpoenas-and-takedown-demands.

21. See "Diebold Coughs Up Cash in Copyright Case," EFF press release, (October 15th, 2004).

22. Ebay Addendum to Notice of Claimed Infringement (NOCI), Reason Code 3.3, available at http://pages.ebay.com/help/tp/vero-rights-owner.html.

23. This dispute most frequently arises in the context of promotional "not for resale" (NFS) and "advance reviewer copy" (ARC) items distributed to members of the media for purposes of review. See the anonymously authored blog article "'Advance review copy: Not for resale' – my ass," The Abstract Factory (May 10, 2006) at http://abstractfactory.blogspot.com/2006/05/advance-review-copy-not-for-resale-my.html.

24. Based on the author's experience with several clients in 2006 and 2007.

25. *Online Policy Group v. Diebold*, 337 F. Supp. 2d 1195 (N.D.Cal. September 30, 2004). The *Diebold* case settled (presumably on the strength of the §512(f) claims) for $125,000 in damages.

26. *Marvel Enterprises v. NCSoft,* 2005 U.S. Dist. LEXIS 8448; 74 U.S.P.Q.2D (BNA) (C.D. Cal. CV 04-9253-RGK Aug. 23, 2005) (action for infringement of rights in comic book characters against company selling online gaming software, where allegedly infringing in-game characers were fashioned by individual users) (officially unreported).

27 *Rossi v. Motion Picture Association of America*, 391 F. 3rd 1000 (9th Cir. 2004).

28. 17 U.S.C. §101, definition of "Work for hire."

29. 17 U.S.C. §107 states that "the fair use of a copyrighted work, including such use by reproduction…for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include— (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copy-righted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work. The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors."

30. *Diebold*, above, Order Granting In Part And Denying In Part Crossmotions For Summary Judgment.

31. See Urban and Quilter, above.

32. *Rossi* at 1005.

33. *Dudnikov v. MGA Entertainment*, 410 F. Supp. 1010 (D. C. Colo. 2005).

34. Dudnikov at 1017.

35 For example, see *Lenz v. Universal Studios* (a Washington Post article discussing the Lenz case can be accessed at http://www.washingtonpost.com/wp-dyn/content/article/2007/10/18/AR2007101802453.html?wpisrc=newsletter&wpisrc=newsletter)

# BUSINESS SOFTWARE ALLIANCE TARGETS MICHIGAN BUSINESSES

**by:** ***Mark G. Malven****

Software compliance watchdog group, the Business Software Alliance (BSA), recently renewed its offer to Michigan residents of up to $200,000 for qualifying software piracy reports. As an organization representing many of the largest software vendors, the BSA operates approximately 65 hotlines around the world for callers who seek information about piracy or who wish to report suspected incidents of software piracy. The BSA takes action against software resellers and end-user organizations that make unauthorized copies of software and works with law enforcement agencies to coordinate enforcement of criminal copyright laws.

With the widespread use of software programs throughout all organizations, those who aren't proactive in their licensing compliance can face significant consequences. The Business Software Alliance often receives its tips from disgruntled employees or former employees (and just about everyone has at least a few people that fit this description). Once that happens most targets should expect to pay a substantial settlement.

As a prophylactic measure, attorneys should be advising all organizations (including non-profits and governments) to regularly undertake a self-audit utilizing automated programs that measure the number of copies of software programs installed and then compare those results to documented licenses purchased. The organization may then fix any non-compliance (by deleting unauthorized programs and/or purchasing the appropriate licenses) before someone contacts the BSA.

In general, the initial BSA demand letter will require an audit and the best approach is to be cooperative at this stage. Once you have the results of the audit, that is where the fun begins. If the gap between the installations and the purchased licenses is significant, one must sometimes get creative with your legal arguments here while still keeping a cooperative tone. In most cases, the client will also need to dig into the facts and search for documents supporting the licenses it has purchased. Resolving these factual issues in your client's favor (as contrasted with making legal arguments denying infringement) is the easier path to lowering your client's exposure.

Ultimately, settling with the BSA will require the payment of a multiple of the unpaid license fees plus legal fees. Failing to settle, however, could lead to a lawsuit alleging copyright infringement under the U.S. Copyright Act, which has provisions and remedies quite favorable to copyright owners. Statutory damages under Section 504(c) of the Act can be as high as $150,000 per program infringed if the infringement is deemed willful. Attorneys fees are also available to prevailing plaintiffs.

In summary, if an organization does receive a demand letter from the BSA, it is very important to involve experienced counsel before responding in any way. The magnitude of the problem, and the size of the potential settlement, can depend significantly on counsel's knowledge of the BSA's methods, tactics and expectations.

**Mr. Malven is the Leader of the Technology Transactions Practice at Dykema Gossett PLLC and was recognized as a Michigan SuperLawyer by the publishers of Law & Politics. He currently serves as the Treasurer of the Information Technology Law Section of the State Bar of Michigan. He has many years experience in the negotiation of technology transactions and the representation of technology-based businesses.*

**LITIGATION SECTION**
STATE BAR OF MICHIGAN
306 TOWNSEND STREET
LANSING, MI 48933-2083

NONPROFIT
U.S. POSTAGE PAID
LANSING, MI
PERMIT NO. 191