An incisivemedia publication

Volume 7, Number 5 • May 2009

Trademark Protection in **Cyberspace Rescued**

By Norman C. Simon

A recent decision of the U.S. Court of Appeals for the Second Circuit, Rescuecom Corp. v. Google Inc., No. 06-4881, F.3d (2d Cir. April 3, 2009), has clarified precedent that had been assumed to foreclose Lanham Act challenges to the surreptitious use of trademarks to compete in cyberspace. In a 2005 decision, 1-800 Contacts v. When U.com, 414 F.3d 400, the Second Circuit dismissed a Lanham Act action against an online marketer because the challenged activity - alleged use of a trademark to generate pop-up Web ads for competitors — was not a "use in commerce" under the statute. District courts uniformly read 1-800 as holding that internal cyber-use of a trademark is never actionable under the Lanham Act. (For more on the 1-800 case, see. "WhenU Helps Keyword Companies See Clearly" in the August 2005 issue of e-Commerce Law & Strategy; www.ljnonline.com/ issues/ljn_ecommerce/22_4/ news/144951-1.html.)

In the wake of *Rescuecom*, that interpretation has been rejected, and advertisers have a potent weapon to protect their trademarks against unfair competition on the Web.

1-800 AND ITS PROGENY

1-800 involved a Lanham Act challenge to the defendant's use of proprietary software to monitor a user's Internet activity for the continued on page 6

Social Media Policies: Your Firm Needs One

By Jay M. Jaffe

doday, our work and personal lives are in a permanent state of collision, and nowhere is that more evident than online in social networks. Chances are, the younger members of your firm grew up managing their personal relationships through MySpace and Facebook — and still do. Now it looks as if the rest of your attorneys and employees are, or will be in the near future, following suit.

In the past few months, Facebook has aged up. According to statistics released by the Web site, the number of Americans over 35, 45 and 55 on Facebook is exploding. In late March, Facebook reported that in the 60 prior days, the number of people on the site over the age of 35 had nearly doubled. In total, about 200 million people are registered users of Facebook.

Social networks in general are experiencing galloping growth. As of February, LinkedIn had more than 35 million registered users. Twitter now has about 10 million users. All are places where people — including your staff — are congregating to share news, insight, maybe a good joke and, if they're not cautious, information that may be damaging to your client relationships or your firm.

NOT IF, BUT WHEN

Even if your law firm hasn't codified the way employees are engaging online, even if your firm doesn't have an official blog, Facebook page or LinkedIn group, even if you're at a firm that blocks access to social networks entirely (and we urge you to reconsider that policy quickly), your employees are already there.

Being engaged in social networks has enormous value for your firm. Through them, you can establish thought leadership, find new recruits, provide a more efficient way for potential clients to find you online, and participate in and monitor discussions about the issues that impact your clients and your firm.

Achieving those benefits, however, requires participation by members of your firm. This group extends beyond your marketing and public relations representatives or a single spokesperson for your firm, all of whom are already well versed in the strategic and prudent disclosure of information. Best practices can be applied continued on page 2

In This Issue

Social Media Policies: Your Firm Needs One. .1 **Trademark Protection In** Cyberspace Rescued . .1 **Existing Internet Laws** Reduce Constitutional Protection3 Twittering in Federal Court.....7

Social Media Policies

continued from page 1

firm-wide that help achieve your business goals and protect the firm. For starters, that means understanding both the legal ramifications of online engagement and the fuzzier, but no less important, implications of the use of the virtual microphone or TV station to enhance your firm's reputation.

The first thing you must do is create a social media policy — or modify an existing policy that is free and available for you to borrow.

How to Build a SOCIAL MEDIA POLICY

At Jaffe, a public relations agency serving only the legal community, we implemented our social media policy over a year ago when we realized that, as communicators, our employees were engaging in online conversations every day. We were conversing with bloggers to promote our clients, and many of us were joining and participating in virtual professional networks, such as Legal OnRamp and LinkedIn. It made sense to us to map out some guidelines for our team.

Last fall, we made our policy available for free downloading through our Web site, www.jaffeassociates. com. You can adapt it as your own or, if you want, comb through the numerous examples of such policies written by organizations such as Sun Microsystems — where thousands of employees have their own blogs the U.S. Navy or Harvard Law School (see, http://twitpwr.com/2Ff/).

Based on our experience at Jaffe, we understood that any company's social media policy should reflect the culture of the firm. For example, Microsoft's social media policy is simply "Be Smart." And, while that may work well for Microsoft, law firms, as you well know, must adhere to different standards.

Jay M. Jaffe is a member of this publication's Board of Editors and President and CEO of Jaffe Associates, a totally virtual PR firm serving only the legal profession. He can be reached at jaffej@jaffeassociates.com.

As well-known://www.dsupra.cogger/docur Kevin O'Keefe recently said in reference to creating a social media policy for a firm's blog: "Apply your existing law firm standards and protocol on confidentiality, PR, marketing, and communication. Who better to know how blogs fit into your culture and the safeguards needed for firm comfort than the firm's own professionals?"

Furthermore, when developing your policy, it's important to be familiar with the ethics rules of the states in which you operate.

WHAT CONSTITUTES WORK-RELATED ACTIVITY ONLINE?

This is a trick question, and a tricky one, given the reality that personal and business worlds are dynamic and constantly bumping into one another, as mentioned above. The answer is that social media policy should apply to work-related online activity; however, what constitutes work-related activity is not black and white.

Take the (completely fictional) example of Leslie Kay, an associate at a firm specializing in bankruptcy law. Leslie is a great lawyer and a rockclimbing enthusiast. For "professional purposes," Leslie has a LinkedIn profile, where she has posted her work experience and titles of books she's reading for work. She even shares information on LinkedIn groups on bankruptcy legal news.

Leslie the rock climber also has a Facebook page where she keeps up with her friends from every stage in her life, including her lawyer and law school friends, and plans outings with a rock-climbing group that communicates through the Web site. Leslie's Facebook profile includes her work information. Leslie also has a blog about rock climbing, and she Twitters when she climbs. Sometimes, Leslie compares her climbs to challenges she faces at work. Leslie's Twitter stream is set to post automatically to her Facebook profile. So while Leslie is using her blog, Twitter and Facebook to pursue her social life, anyone who wants to can

continued on page 4

TNERNETS 464 6345bcf5 45 55d5 476 f348 220 βa9960ce6

Steven Salkin, Esq.

& STRATEGY®

EDITORIAL DIRECTOR Wendy Kaplan Ampolsk

EDITOR-IN-CHIEF

MANAGING EDITOR

Jeannine Kennedy Louis F. Bartella GRAPHIC DESIGNER BOARD OF EDITORS ROBERT J. AMBROGI Rockport, MA BRITT L. ANDERSON. Manatt, Phelps & Phllips San Francisco IOHN T. AQUINO Washington, DO Wolf, Greenfield & Sacks, P.C. Roston JONATHAN BICK Of Counsel, WolfBlock Brach Eichler Roseland, NI Adjunct Professor of Internet Law Rutgers School of Law Pace University Law School RIITH HILL BRO Baker & McKenzie, LLP Chicago PETER BROWN Baker & Hostetler, LLP EVAN R. COX..... Covington & Burling LLP San Francisco VICTORIA A. CUNDIFF. Paul, Hastings, Janofsky & Walker New York STEPHEN W. FEINGOLD . . . Day Pitney LLP MICHAEL GEIST Univ. of Ottawa Osler Hoskin & Harcourt, LLP Ottawa, Canada Gray Matters MEGAN E. GRAY Washington, DC
MARK GROSSMAN Law Offices of Mark Grossman, P.A. Coral Gables, FL MARCELO HALPERN..... Latham & Watkins Chicago JAY M. JAFFE..... Jaffe Associates, Inc. Washington, DC
SEAN F. KANE Drakeford & Kane, LLC New York CATHERINE S. KIRKMAN. . . . Wilson Sonsini Goodrich & Rosati Palo Alto, CA JEFFREY R. KUESTER. Thomas, Kayden Horstmeyer & Risley, LLP Atlanta MARTIN H LEVENGLICK Morrison Cohen LLP

CHARLES R. MERRILL.... McCarter & English, LLP Newark, NJ . Eckert Seamans Cherin & RICHARD E. PEIRCE Mellott, LLC

New York

New York

Philadelphia PROF. HENRY H. Chicago-Kent College of Law

BENNETT M. LINCOFF

Chicago
MICHAEL G. RHODES. Cooley Godward, LLP San Diego Kelley Drye & Warren LLP LEWIS ROSE..... Washington, DC . Morris, Manning & Martin F. LAWRENCE STREET

Atlanta Kasowitz, Benson, Torres, and Friedman LLP

New York CYDNEY A TUNE Pillsbury Winthrop Shaw Pittman

San Francisco DOUGLAS WOLF..... Wolf, Greenfield & Sacks, P.C. Boston

E. ROBERT YOCHES Finnegan, Henderson, Farabow, Garrett & Dunner, LLP Washington, DC

Internet Law & Strategy® (ISSN 1-57786-181-7) is published by Law Journal Newsletters, a division of Incisive Media. © 2009. Incisive US Properties, LLC. All rights reserved. All rights reserved. No reproduction of any portion of this issue is allowed without written permission from the publisher. Telephone: (877) 256-2472 Editorial e-mail: steve.salkin@incisivemedia.com Circulation e-mail: customercare@incisivemedia.com Reprints: reprintscustomerservice@incisivemedia.com

> Internet Law & Strategy USPS Number 021967 Periodicals Postage Paid at Philadelphia, PA POSTMASTER: Send address changes to: Incisive Media 120 Broadway, New York, NY 10271

Published Monthly by: Law Journal Newsletter 1617 IFK Boulevard, Suite 1750, Philadelphia, PA 19103



Existing Internet Laws Reduce Constitutional Protections

By Jonathan Bick

Internet communication necessitates sharing content and data with third parties. The voluntary transfer of such content and related data to third-party Internet communication facilitators reduces or eliminates First, Third, Fourth, Fifth and Fourteenth Amendment rights of Internet users. The technology and protocols used to enable Internet communication, as interpreted by existing privacy statutes and case law, further compromises Internet users' privacy and publicity rights. Both legal notices and technological techniques may be used to ameliorate this outcome.

THIRD PARTIES REQUIRED

While the Internet appears to be complex with a myriad of communication lines, it is not. The Internet is a relatively simple and redundant system that transmits data from one available computer to another using a procedure requiring that content and data be duplicated by third parties all along the way.

In particular, the Transmission Control Protocol ("TCP") and the Internet Protocol ("IP") are required of all Internet communication and oblige all Internet messages to be sent in a specific manner. All computers sending Internet messages must first enclose them in uniquely addressed digital envelopes, then send them to the gateway computer to be handed off to other networks. Each computer handles each Internet message by copying and routing such encapsulated IP packets from network to network.

Historically, the American privacy doctrine is modeled upon real property concepts. Since the Fourth Amend-

Jonathan Bick, a member of this newsletter's Board of Editors, is an adjunct professor of Internet law at Pace Law School and Rutgers Law School. He is also the author of 101 Things You Need To Know About Internet Law [Random House 2000].

ment has been/wincreasingly/psubjectment/ingly/spexiousses.bdg-5478-9448-7203a9960ce6 to codification, most modernization of privacy law is a function of legislative action. As a consequence, such changes are dependent upon political, rather than technological, change. No such change has yet been implemented with respect to Internet privacy.

PRIVACY INTEREST, NOT RIGHT

There is no explicit right to privacy in the United States Constitution. The Supreme Court has found several privacy interests, including:

- The right of association contained in the First Amendment;
- The Third Amendment's privacy right of a home owner by its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner;
- The Fourth Amendment explicitly affirms the privacy right of people with respect to their persons, houses, papers and effects, against unreasonable searches and seizures:
- The Fifth Amendment's zone of privacy which government may not force one to surrender detrimental information; and
- The Fourteenth Amendment's application of privacy rights to the states.

In short, the Supreme Court's findings are protections against all governmental invasions of life's privacies.

Just as there is no explicit constitutional right to privacy, there is no general privacy statute that requires electronic records held by third parties to keep such records private. Rather, the protection of such electronic records may be found due to a particular set of facts.

THE FOURTH AMENDMENT

Two approaches to Fourth Amendment privacy protection are generally used. One approach equated unlawful requests for information with unlawful search and seizure. The other approach required physical trespass into a zone of privacy. Katz v. United States, 389 U.S. 347 (1967). But the Katz court recognized that the "Fourth Amendment protects people, not places. What a person knowin his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."

In short, the Supreme Court has found that capacity to claim the protection of the Fourth Amendment depends upon whether the person who claims the protection of the amendment has a legitimate expectation of privacy in the invaded place. See, Rakas v. Illinois, 439 U.S. 128, 143 (1978). However, a subjective expectation of privacy is legitimate if it is one that society is prepared to recognize as reasonable, according to Minnesota v. Olson, 495 U.S. 91 (1990).

Thus the privacy interest one retains in information transmitted to a third party is clear. Courts have found no reasonable expectation of privacy; they have highlighted factors evidencing consent. In Smith v. Maryland, 442 U.S. 735, 742 (1979), the Supreme Court found that there is no such expectation of privacy regarding the numbers dialed on a telephone because the telephone company was expected to access the information. Similarly, in *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000), the court found that an employee did not have a legitimate expectation of privacy with regard to his employer's record of his Internet usage.

PRIVACY OF THE NET

Due to the Internet's system of transmitting data from one relatively available and local computer to another, using a protocol of transmission which requires that content and data be duplicated by third parties all along the way, it may be argued that there is no reasonable expectation of privacy in Internet communications.

At least three courts have attempted to grant some Internet privacy on the grounds that it may be reasonably expected. See, United States v. Maxwell, 45 M.J. 406, 417 (1996), which found that the tenor and content of the e-mail conversations between appellant

Internet Laws

continued from page 3

and his correspondent suggested that they each had an expectation that the conversations were private. Similarly, in Warshak v. United States, 490 F.3d 455, (6th Cir. 2007), the court found a reasonable expectation of privacy in e-mail communications after narrowing the inquiry to identify the party with whom information was shared or from whom information was shielded, and the precise information actually conveyed. Also, the court in United States v. Heckenkamp, 482 F.3d 1142, 1147 (9th Cir. 2007), found that a student had a reasonable expectation of privacy in information he transmitted over the university's network insofar as there was no announced monitoring policy.

In Berger v. New York, 388 U.S. 41 (1967), the Supreme Court defined the procedural safeguards necessary to protect the privacy interest. In particular, once a user establishes such a reasonable expectation of privacy, the inquiry shifts to whether the statute at issue sufficiently protects that right to privacy. To date, no such shift has occurred.

The Electronic Communications Privacy Act of 1986 ("ECPA"), 18 U.S.C. §§2510-2521, 2701-2711, 3121-3127 (2006), extends government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer. However,

the ECPA only protects wire, oral and electronic communications while in transit. Internet communication technology and protocols mandate that Internet messages stop and be stored multiple times en route, thus eliminating the application of ECPA to Internet communication.

OVERCOMING DIFFICULTIES

To overcome some of the difficulties inherent in Internet communication, both technological and legal options are available. Both options attempt to either limit the amount and change the nature of content and data available to third parties or change the privacy expectation by providing notice.

First, an Internet user may employ legal notices to change the expectation of privacy with respect to the Internet communication. In particular, an Internet user may embed a notice in the communication putting a thirdparty recipient on notice that the communication is privileged, proprietary or confidential — and that the third party should treat it as such. Just as it is important to place a notice on a fax cover sheet, it is important to use technology to ensure that the notice appears prior to allowing a third party access to the Internet communication data or content. The use of data formatting to prevent deep linking can be employed to force a thirdparty reader of an Internet communication to view the beginning of an Internet communication before being able to access any other part.

Next, an Internet user may use te mentViewer.aspx?fid=6345bcf5-55d5-476f-848c-7203a9960ce6 nology to limit a third party's access

to the content of the communication. For example, a privileged, proprietary or confidential Internet communication may be sent as an attachment. The disclaimer in the body of the e-mail might then read: "The attachment to this e-mail may be privileged, proprietary or confidential. Do not open it. It is intended only for the e-mail recipient noted above. If you are not the intended recipient or a person responsible for delivering this transmission to the intended recipient, you may not disclose, copy or distribute this transmission or take any action in reliance on it."

Additionally, the communication may be password protected or encrypted. Rather than using exclusively random public Internet communication servers, an Internet message may be sent using some private or specified Internet communication servers.

Since technological developments outpace the rate of legal evolution, digital networks can no longer be wiretapped like analog phone systems. Future legislatures are likely to enact laws that prohibit governmental entities' access in counterintuitive ways, especially where the parties involved, the content and the nature of the communication are unknown. However, such is currently not the case.



Social Media Policies

continued from page 2

find out where she works and then find Leslie on LinkedIn.

If an employee mentions on a personal social network profile that she works for your firm, then the social media policy can apply to her activity in social networks.

THE COMMON SENSE CLAUSE

Here's how we handled this dilemma in the Jaffe Associates social media policy:

You are responsible for what you post. You are personally responsible for any of your on-

line activity conducted with a firm e-mail address, and/or which can be traced back to the firm's domain, and/or which uses firm assets. The (FIRM DO-MAIN).com address attached to your name implies that you are acting on the firm's behalf. When using a firm e-mail address or firm assets to engage in any social media or professional social networking activity (for example LinkedIn and Legal OnRamp), all actions are public, and attorneys (and staff) will be held fully responsible for any and all said activities.

THE LESS THAN **OBVIOUS CLAUSE**

Outside the workplace, your rights to privacy and free speech protect online activity conducted on your personal social networks with your personal e-mail address. However, what you publish on such personal online sites should never be attributed to the firm and should not appear to be endorsed by or originated from the firm. If you choose to list your work affiliation on a social network, then you should regard all communication on that network as you

Social Media Policies

continued from page 4

would in a professional network. Online lives are ultimately linked, whether or not you choose to mention the firm in your personal online networking activity.

Some companies solve the problem by asking their employees who blog to name their employer on the blog, whether the blog relates to business or not. Other companies ask that employees post a disclaimer that indicates that the views on the site are not necessarily those of the company. Social media guru and uber-blogger Robert Scoble, who blogs on Scobelizer.com, has just such a clause on his blog.

SO WHAT CAN EMPLOYEES POST?

At their core, social media policies are there to encourage, rather than discourage, activity on social networks. Social networks are meant to be conversations, and that's a very good thing. It shows the human face of your firm.

In general, posting policies should follow common sense:

- Don't post anything that's confidential;
- Avoid the appearance of establishing a client-attorney relationship;
- Don't get into an argument with anyone; and
- Be polite and avoid sensitive subiects.

But the truth is, younger employees have been online for years, sharing everything they can think of (and things you may not have) and aren't used to putting on the brakes, even when it comes to engaging in conversations online on behalf of work.

One intriguing policy is Sun Microsystems', which starts by assuming that its employees will use common sense, but also offers some suggestions on how to dive in.

The lessons garnered from Sun are: Be respectful, never identify anyone in a photo or quote someone unless he or she has given you express permission to do so and be transparent. Lay claim to your posts and comments. (*See*, www.sun.com/communities/guidelines.jsp.)

Creating a fake identity or posting anonymously can have serious consequences. Whole Foods suffered when its president, John Mackey, used a fake identity to post questions on Yahoo! As reported in the August 2007 issue of Internet Law & Strategy: "So goes the strange tale of John Mackey, the chief executive officer of Whole Foods Market, who used a pseudonymous identity on the Yahoo! message boards for nearly eight years to lambaste competition and promote his supermarket chain's stock, according to documents released by the Federal Trade Commission (FTC). ... Many of the messages he sent as 'Rahodeb' were critical of Wild Oats Markets, Inc., which Whole Foods is trying to acquire. The postings came to light in documents filed by Whole Foods with the FTC, which is seeking to block the Wild Oats acquisition. ... The [Securities and Exchange Commission] will decide whether to proceed with a formal investigation delving into Mackey's 'sock-puppeting' shenanigans as 'Rahodeb,' which, in retrospect, may prove to have been a costly hobby that derailed a profitable acquisition for Whole Foods, and caused an embittered man to sue his Wild Oats." (See, www.ljnon line.com/issues/ljn internetlaw/5 8/ news/149056-1.html.)

MAINTAINING CLIENT CONFIDENTIALITY

It almost goes without saying that a breach of confidentiality would have a serious impact on your firm. This needs to be clearly spelled out in any social media policy, because such breaches may be unintentional. Once something is out there on the Web, it can be spread — and repurposed — anywhere.

Here's how we provide guidance in the Jaffe Associates' social media policy:

Avoid forums where there is little control over what you know to be confidential information. In the world of social networking, there is often a breach of confidentiality when someone e-mails an attorney or posts a comment congratulating him/her on representation of a specific client or on a specific case. Often these

ewer.asbx?fid=6345bcf8-55d5-476f-848c-7203a99 social network circles — it's how attorneys are establishing credibility — so be very selective and thoughtful about where you post and how you reply (or not).

SHOULD APPROVAL BE REQUIRED BEFORE EMPLOYEES POST?

Generally, if a social media policy is in place and the firm's staff is trained in how to engage online, the vast majority of posts should not require approval by anyone else in the firm. In fact, employees who are already using social networks may balk at this oversight and significantly scale back their participation online. The purpose of a social media policy should not be to squash online engagement.

There will be times, however, when such approvals are necessary. These include occasions when employees wish to respond to a negative or inaccurate post about your firm or a client, post recommendations for colleagues (which can be perceived as testimonials) or respond directly to journalists regarding issues of concern for the firm. All of these instances can have unintended legal repercussions.

WHY YOU MAY WANT TO HAVE A DISCLAIMER

For lawyers, it's important to be very clear about what is - and isn't - offered on social networks. The vast majority of social media experts in the legal field advise that firms use disclaimers on their blogs, especially when communicating about fees, awards, recent cases or case outcomes, or when offering information. That's because attorney-client relationships may be created online; this often occurs in social media whether you want it to or not. To protect your firm, disclaimers may be prudent. As we note in Jaffe Associates' social media policy:

Some firms are building in popup boxes that stop people from emailing an attorney and require them to accept the terms of a disclaimer before e-mailing information that could constitute an attorney-client relationship.

Social media policies can help protect the firm's reputation. But having such a policy and implementing

Trademark Protection

continued from page 1

purpose of generating advertising. The plaintiff alleged that the defendant committed trademark infringement by generating a "pop-up ad" for a competitive product every time a user accessed the plaintiff's Web site. The district court preliminarily enjoined the defendant from the practice.

On interlocutory appeal, the Second Circuit vacated the injunction, holding as a matter of law that the defendant had not "used" the plaintiff's trademark "in commerce," as required by the Lanham Act. Specifically, the court observed that the defendant had "not use[d] 1-800's trademark in the manner ordinarily at issue in an infringement claim," that is, by placing the mark on goods or services in order to pass them off as emanating from or authorized by 1-800.

In the wake of 1-800, several district courts in the Second Circuit dismissed attempts by trademark owners to use the Lanham Act to combat the unauthorized use of their marks in cyberspace. These courts reasoned that under 1-800, the internal computer use of a trademark is not actionable as a "use in commerce." For example, in S&L Vitamins Inc. v. Australian Gold Inc., 521 F.Supp.2d 188 (EDNY 2007), the court held that utilizing a competitor's trademark in a metatag to influence search engine results did not constitute a "use" within the meaning of the Lanham Act. (See also, FragranceNet.com Inc. v. FragranceX. com Inc., 493 F.Supp.2d 545 (EDNY 2007) (no trademark "use" based on defendant's utilization of plaintiff's trademark as search engine keyword or as metatag); Merck & Co. Inc. v. Mediplan Health Consulting Inc., 425 F.Supp.2d 402 (SDNY 2006) (internal use of trademark as keyword to trigger "sponsored links" to defendants' Web sites was not placement of trademark on goods and thus not actionable "use").

Norman C. Simon is a litigation partner with Kramer Levin Naftalis & Frankel. **Carl D. Duffield**, a litigation law clerk with the firm, assisted with the preparation of this article.

1-800 LIMITED TO WEAGUE TO ACCOM/POST/docume/Prosite at the South of the Act and 1203a9960ce6

The district court in Rescuecom likewise reasoned that 1-800 mandated the dismissal of plaintiff's trademark infringement, false designation of origin and dilution claims. In Rescuecom, Plaintiff challenged Google's sale of the "Rescuecom" trademark as a keyword in its AdWords service, which allows advertisers to purchase terms that generate "sponsored links" in response to a Web search. Plaintiff alleged that "whenever a user launches a search for the term 'Rescuecom,' seeking to be connected to Rescuecom's Web site, the competitors' advertisement and link will appear on the searcher's screen ... allow[ing] Rescuecom's competitors to deceive and divert users searching for Rescuecom's [W]eb site."

The lower court dismissed under 1-800 because the non-visible use by Google of the "Rescuecom" trademark was not an actionable "use in commerce." The Second Circuit vacated and remanded, adopting an extremely narrow view of 1-800, effectively abrogating the case to its unique factual posture. Two material factual differences between the cases were deemed critical.

First, the court reasoned that the defendant in 1-800 did not use the plaintiff's mark, but instead its Web site address. The Rescuecom court viewed this to be a critical distinction, observing that the "[W]eb site address was not used or claimed by the plaintiff as a trademark," and "[t]he question whether the plaintiff's [W]eb site address was an unregistered trademark was never properly before the 1-800 court." A footnote added the caveat that "[w]e did not imply in 1-800 that a [W]eb site can never be a trademark" and "[i]n fact, the opposite is true." A practical implication is that advertisers should take care to federally register their domain names to ensure that they will have trademark protection.

Second, the *Rescuecom* court explained that the defendant in *1-800* did not use, display or sell the plaintiff's mark. The pop-up ad at issue was controlled by a category associated with the Web site — for example, "eye care" — rather than the

sell any trademarks to others. Thus, the *Rescuecom* decision explained: "To the extent that an advertisement for a competitor of the plaintiff was displayed when a user opened the plaintiff's [W]eb site, the trigger to display the ad was not based on the defendant's sale or recommendation of a particular trademark." In contrast, Google allowed others to buy the "Rescuecom" mark as a keyword, an activity that fit within the Lanham Act's required "use in commerce."

AMICI'S ARGUMENTS REJECTED

The Second Circuit accepted four amicus briefs — two by consumer advocacy groups, one by a group of law school professors, and one by other Internet service providers — that all joined Google in urging affirmance of the dismissal of Rescuecom's complaint. The Second Circuit considered and rejected two arguments advanced by *amici* and by Google.

Marshaling the uniform interpretation of 1-800 by district courts in the circuit, Google and its amici argued that as a matter of law, "the inclusion of a trademark in an internal computer directory cannot constitute trademark use." This argument hinged on language in 1-800 that the "internal utilization of a trademark in a way that does not communicate it to the public is analogous to an individual's private thoughts about a trademark," and therefore is not actionable under the Lanham Act. The Rescuecom court flatly rejected this argument, stating that it "overreads the 1-800 decision." The court further explained: "We did not imply in 1-800 that an alleged infringer's use of a trademark in an internal software program insulates the alleged infringer from a charge of infringement, no matter how likely the use is to cause confusion in the marketplace."

The Second Circuit's clarification harmonizes its view with that of other circuits that have considered the issue. See, North Am. Med. Corp. v. Axiom Worldwide Inc., 522 F.3d 1211 (11th Cir. 2008) (use of trademark in metatag constitutes "use in commerce"); Brookfield Commc'n. Inc. v. West. Coast Entm't Corp., 174 F.3d 1036 (9th Cir. 1999) (same). Indeed, the U.S. Court

Twittering in **Federal Court**

By Lynne Marek

Some federal judges are opening the door to the press reporting directly from their courtrooms in the interest of bringing more transparency to the judicial process.

Judge Tom Marten of the U.S. District Court for the District of Kansas in March allowed a reporter for the Wichita Eagle to send Twitter messages directly from the courtroom where a trial of gang members was under way. Judge Mark Bennett of the U.S. District Court for the Northern District of Iowa also this year allowed blogging from his courtroom in the trial of a landlord who pleaded guilty to fraud, but went to trial on income tax violations.

Many federal court judges have barred the use of electronic devices in their courtrooms, prohibiting everything from laptops to handheld devices that can send electronic messages, often in the interest of insulating jurors from media coverage to ensure a fair trial for defendants. Judges have also been concerned about the potential disruption to their courtroom proceedings. Still, the U.S. Judicial Conference has no formal policy on the matter, leaving such questions up to individual judges.

"We're by choice the most mysterious and least transparent branch of government, and I think we have an obligation to be more transparent," Bennett said.

Lynne Marek is a staff reporter for the National Law Journal, an Incisive Media affiliate of Internet Law & Strategy.

Social Media Policies

continued from page 5

it properly requires careful attention to the nuances of the rapidly changing online world. When everyone is encouraged to dive in and converse, when it's so easy to demonstrate expertise and to share, it's easy to go over the line and, for example, answer

Document hosted at JDSUPRA While the replace by the second of the second ging from some other high-profile federal trials, including that of I. Lewis "Scooter" Libby, former chief of staff to former Vice President Dick Cheney, in Washington, and newspaper publisher Conrad Black in Chicago, those dispatches were not made directly from the courtrooms, and such coverage would have been prohibited at those courts. Variations among federal courts on such rules have existed for years with some federal courts, such as the U.S. District Court for the Eastern District of Arkansas, allowing reporters to use tape recorders in courtrooms (the tape recorders are for the reporters' own use, not for broadcast).

Marten and Bennett both allowed the coverage after the individual reporters approached them and asked about doing it. Marten said he has known Ron Sylvester, the Wichita Eagle reporter Twittering from his courtroom, for years and respects his reporting, but would likely extend the same privilege to other reporters too. The judge said he was quickly able to overcome one defense lawyer's concerns that jurors might breach court rules to view the reporting and be inappropriately swayed.

"You either trust jurors to honor the admonishment or not," Marten said. "This was pretty much a nonissue. I don't see any difference between this and a journalist sitting in there taking notes."

Sylvester has also been allowed to send such messages during coverage of cases in Kansas state court trials. State courts also have a patchwork of policies with some, including Illinois, barring communication such as Twitter from a courtroom, and

a legal question on a social network such as Facebook or LinkedIn. More important than any social media policy, then, is training staff on best practices in social media, asking for their participation and keeping up with the changes in the technology and new media so that you can help the firm stay apace and reputable.

To say that social networking is counterintuitive to the practice of ing such decisions up to individual iudges.

When one New York judge came to David Bookstaver, communications director for that state court system, to voice a concern about reporters coming and going from his courtroom during the Christie Brinkley divorce trial last year, Bookstaver told him the disruption could be eliminated by allowing the use of BlackBerry devices. The judge took his advice.

"It goes to a judge controlling his or her courtroom," Bookstaver says, noting that he has reminded judges and court officers alike that the New York system doesn't bar the devices. "I think this is a matter of changing a culture, not only with the judges but with the court officers."

The use of such technology in the courtroom will become more accepted as a younger generation of judges that is less affected by media attention and more technologically savvy takes their places on the bench, says Judge Marten, who is 57. Bennett, the Iowa federal judge, is 58.

"We are moving to a time when there is more rather than less access to the courtroom by what judges view as non-intrusive elements of the press or public," says First Amendment specialist Floyd Abrams, a partner at New York-based Cahill, Gordon & Reindel.

The reason some federal judges fear allowing electronic messaging from their courtrooms is that they believe it will lead to other types of coverage they consider more intrusive, such as TVs in the courtrooms, Abrams says. "There are a number of judges afraid of the slippery slope."

--&-

law is an understatement. And to say that a social networking policy will be the panacea that will solve all issues that arise in this brave new world is naïve. A social networking policy obviously is a great starting point, but only if you understand that all of the rules may change by the time you read this article.



Trademark Protection

continued from page 6

of Appeals for the Eleventh Circuit recently criticized 1-800, observing that to the extent it "based its 'use' analysis on the fact that the defendant did not display the plaintiff's trademark, we think the Second Circuit's analysis is questionable." Axiom Worldwide, 522 F.3d at 1219.

The Rescuecom court also rejected a second argument advanced by Google and its amici that urged that the use of the Rescuecom mark to generate sponsored links was the cyberspace equivalent of "product placement" in the brick-and-mortar world. An example of product placement is when a generic product is shelved adjacent to a branded product with the intent that consumers seeking out the trademarked product will instead consider purchasing the less expensive generic alternative. Google's use of Rescuecom's trademark to list competitors' Web sites along with the plaintiff's site in search engine results was argued to be the online equivalent.

The Rescuecom court concluded that the analogy was flawed because if consumer confusion was the likely result, even ordinary product placement was actionable under the Lanham Act. "If a retail seller were to be paid by an off-brand purveyor to arrange product display and delivery in such a way that customers seeking to purchase a famous brand would receive the off-brand, believing they had gotten the brand they were seeking, we see no reason to believe the practice would escape liability merely because it could claim the mantle of 'product placement."

Accepting the allegations in the complaint as true, as it was required to do on a motion to dismiss, the Rescuecom court concluded that Google's practice was "significantly different from benign product placement that does not violate the [Lanham] Act." The court emphasized, however, that "[w]e have no idea whether Rescuerant proventhat/document/newer asply and 63 sports 55 and 61 4450 7203 as 9960 ce6 Google's use of Rescuecom's trademark in its AdWords program causes likelihood of confusion or mistake."

Rescuecom might very well have a challenging time making this showing — at least as it relates to Google. As one amicus explained, Google is not responsible for the content of search results generated by the term Rescuecom. Google also prominently identifies as "sponsored links" those results yielded from purchased keywords, thereby signaling to the public that they constitute paid advertising and helping to reduce the likelihood of confusion.

A Postscript

The Rescuecom court also took the unusual step of issuing an appendix to correct a flaw in the 1-800 decision's statutory interpretation. While stressing that the 1-800 holding "was justified by numerous good reasons and was undoubtedly the correct result," the Rescuecom court pointed out that, nevertheless, it relied in part on two district court opinions from other circuits that "overlook[ed] key statutory text" of the Lanham Act. The appendix provides an elaborate history of the evolution of the phrase "use in commerce" in different sections of the Lanham Act.

The Rescuecom court explained that 1-800 cited district court decisions relying on that part of the definition of "use in commerce" in 15 USC §1127 providing that a mark "shall be deemed to be in use in commerce ... on services when it is used or displayed in the sale or advertising of services and the services are rendered in commerce." What those decisions, and hence the 1-800 court overlooked, however, was that the first sentence of the definition in §1127 requires the "bona fide use of the mark in the ordinary course of trade, and not made merely to reserve a right in the mark."

The Rescuecom court concluded that this definition could not apply to those sections of the statute governing infringement and false adverbecause "[i]f §1127's definition is applied to the definition of conduct giving rise to liability in §§1114 and 1125, this would mean that an accused infringer would escape liability, notwithstanding deliberate deception, precisely because he acted in bad faith."

It was "inconceivable" that Congress could have intended this result; rather, it was "clear Congress did not intend that this definition apply to the sections of the Lanham Act which define infringing conduct." The Second Circuit thus opined that the entire definition in §1127, including the bona fide use requirement, should apply to "use in commerce" as it relates to trademark registrations. The definition of "use in commerce" in the infringement context, however, should be governed exclusively by reference to the second sentence.

In the end, even though "the judges of the 1-800 panel read [the] Appendix and authorized [the Rescuecom panel] to state that they agree with it," the Rescuecom court emphasized that it was "dictum and not a binding opinion of the court." The Second Circuit expressly invited Congress to "study and clear up this ambiguity" in the definition of "use in commerce" in the Lanham Act.

CONCLUSION

The Second Circuit's reversal in Rescuecom by no means assures a victory for the plaintiff on the merits. Having survived the motion to dismiss, Rescuecom must prove likelihood of consumer confusion before it is entitled to relief under the Lanham Act. Nevertheless, this recent decision arms advertisers with the means to combat unfair competitive cybermarketing practices.



The publisher of this newsletter is not engaged in rendering legal, ting, financial, investment advisory or other professional servic es, and this publication is not meant to constitute legal, accounting, financial, investment advisory or other professional advice. If legal, financial estment advisory or other professional assistance is required, the services of a competent professional person should be sought.

To order this newsletter, call:

1-877-256-2472

On the Web at:

www.ljnonline.com