Intellectual Property

2007 FALL BULLETIN

Secrets Easily Leaked by Friend or Foe in Publicly Filed .PDF Documents

BY ROBERT D. BROWNSTONE, TODD R. GREGORIAN, AND MICHAEL A. SANDS

Introduction — The Dangerous Landscape

Disclosures to government regulators have always posed risks to trade secrets and other proprietary information. It came as little surprise, therefore, when the Federal Trade Commission's mishandling of confidential information in its antitrust challenge to the merger of Whole Foods and Wild Oats came to light in an Associated Press (AP) article. *See, e.g.,* Christopher S. Rugaber, *Error by FTC Reveals Whole Foods' Trade Secrets* (AP Aug. 15, 2007).

I. FTC's Leakage of Whole Foods' "Under Seal" Information

Unsound electronic redaction in *FTC v. Whole Foods Market and Wild Oats Markets*, Civ. No. 07-cv-01021-PLF (D.D.C. June 5, 2007) resulted in an electronically-filed FTC brief exposing significant operational and strategic business information considered confidential by Whole Foods. By the time the court discovered the error, the national press had already obtained a copy of the brief. Too late for Whole Foods, the FTC filed a corrected copy that had been printed to paper and scanned into image format.

The District Court's August 16, 2007 order denying the FTC's motion for a preliminary injunction did not mention the redaction error. In fact, the order praised both sides for litigating the matter on a tight schedule. The FTC's disclosure appears not to have prejudiced either side with respect to the merits of the merger challenge. However, it remains to be seen whether Whole Foods faces negative blowback from its aggressive stance towards competitors or site-selection criteria revealed by the FTC's error.

The mistake made by the FTC was basic. In preparing its brief for filing, FTC staff wrongly assumed that the metadata in its word processing file would not migrate upon direct conversion from native format to portable document format (.pdf). In particular, they wrongly assumed that using Microsoft's "Highlight" (or "Borders and Shading") tool to black out text actually *removed* the text from the file's contents. It does not. It "covers up" the text, but the text itself remains in the file, fully searchable and available for copying. The resulting .pdf appears at first glance to contain only black boxes in place of the redacted content. That content, however, is present in the .pdf file and can be easily revealed either by copying and pasting the blacked-out text into a word-processing file or an e-mail message or by viewing the .pdf file in a reader such as Preview or Xpdf.

II. Similar Prior Well-Publicized Mishandlings of Redactions and Metadata

The FTC is not the first litigant to make this type of mistake to the detriment of another party. Redaction *faux pas* and other types of metadata-handling errors are, regrettably, fairly common. Famous entities bitten by the metadata cobra in recent years include the United Nations, the British Prime Minister's Office (via the "Downing Street Memo"), the current Republican administration, the Democratic National Committee, the California Attorney General's Office, the Motion Picture Association of America, and SCO Group. *See, e.g.,* Tom Zeller Jr., *Beware Your Trail of Digital Fingerprints*, N.Y. Times (Nov. 7, 2005).

In This Bulletin

Fenwick
FENWICK & WEST LLP

The publicized snafu most analogous to the FTC's recent error occurred in May 2006, in a case filed by various civil liberties groups challenging National Security Administration surveillance activity. In *Hepting, et al. v. AT&T,* 439 F. Supp. 2d 974 (N.D. Cal. 2006), a law firm representing AT&T filed a redacted reply brief suffering the same deficiency as the FTC's *Whole Foods* brief. That reply brief — still posted on multiple websites — listed potential uses (aside from allegedly illegal, NSA-requested surveillance) AT&T might have for a "secret" switching room designed to monitor telephone calls and internet transmissions. That disclosure was especially ironic given the NSA's recent prior publication of *Redacting with Confidence: How to Safely Publish Sanitized Reports Converted From Word to PDF* (Feb. 2, 2006).

One month later, in June 2006, a brief filed in connection with the investigation of leaked grand jury testimony from the BALCO steroid case also contained faulty redactions. That gaffe had resulted in disclosure of eight pages of e-mails between Victor Conte, the primary criminal defendant, and Mark Fainaru-Wada, a Chronicle reporter whose articles had referenced the leaked materials. The emails show Fainaru-Wada aggressively pursuing a CD-ROM containing the record of the grand jury proceedings. *See, e.g.,* Adam Liptak, *Prosecutors Can't Keep a Secret in Steroid Case*, N.Y. Times (June 23, 2006).

III. Proper Methods of Redaction

Fortunately the redaction error made in those cases is easily avoided under a variety of methods, one or more of which ideally should be adopted as a strict protocol at the outset of a proceeding. Here is just one such protocol for Office 2003 users in the e-filing context:

(1) Make sure that the applicable local rules, "under seal" order or judge's procedures actually require e-filing a redacted version of the document (as opposed to just filing a physical copy at the clerk's office and/or in chambers).

(2) *Do not* use the "Highlight" or "Borders and Shading" features in Word for redactions (unless you then print the document to paper and scan it into an image file), instead:

   (a) Download and install the "Word Redaction" tool from the Microsoft website.

   (b) Copy the Word file that is to be redacted, and once in the copy, follow the instructions provided with the "Redaction" tool.

   (c) Use metadata-removal software to clean (a.k.a. "scrub") file-system data and embedded data from the redacted copy.

   (d) Convert the redacted, scrubbed copy of the Word file to .pdf.

Adobe® Acrobat® 8 Professional now has its own redaction tool, which may also provide a workable solution to this problem. One "low-tech" solution is to print the document to paper, redact the confidential portions manually with black marker or cover-up tape and then scan the document into an image file. If necessary, text-searching – as well as copy-and-paste capability – can be restored to a scanned document using OCR software or Acrobat's "Capture" feature. Alternatively, Word's "Highlighter" or "Borders/Shading" feature – or any electronic redaction tool — can be used prior to printing. Either way, the scan of the paper printout will not retain the metadata from the original file.

Even after a protocol is established and adopted by litigants, there remains the hurdle of the court's own procedures. A separate source of disclosure risk is the court itself, typically the most overburdened and understaffed participant in the litigation process. Disclosure may occur via an inadvertent mention on the record at a hearing or a reference in a written order. In *Whole Foods*, the court's novel solution to the latter problem was to provide a non-public draft order to the parties and have them lodge suggested redactions with chambers prior to the release of the public version. Other courts may be willing to take similar precautions, but the onus likely will be on parties desiring such relief to make the court aware of the issue and affirmatively seek help. Litigants concerned about safeguarding confidential information should not presuppose *sua sponte* protective action by courts struggling to get through their dockets.

Conclusion

Ultimately, litigants and entities facing government inquiry are always susceptible to risks associated with mistreatment of their confidential information. Often, disclosures result from simple inadvertence regarding the nature of the information itself. The above examples of technological mistakes are especially vexing, however, because the attorneys in question both recognized the need for confidential treatment and implemented a method that they believed would effectively protect the confidence. Regrettably, this type of disclosure is likely to be just as persistent — and as damaging — as plain inadvertence or even an intentional violation. As document-generating software and other technological tools used by parties and regulators are constantly updated — with new holes appearing in each subsequent version — generating a one-size-fits-all protocol may prove difficult, if not impossible. For now, at least, the suggestions discussed above will help avoid the most egregious forms of mistaken disclosures.

Screen Scraping: How to Use a Bot and Not Get Busted

BY BRIAN CARVER

Screen scraping is any automated process for extracting content from a website for use in another context. Screen scraping is acomplished using programs called robots, web-crawlers, spiders, or just bots.

Search engines also deploy bots to crawl the web, but most retrieve primarily static content and visit a given website somewhat infrequently, placing very little burden on the sites visited. The bots that typically cause trouble seek out dynamic content in response to user inputs and visit the targeted site repeatedly, sometimes contributing significantly to the visited site's overall traffic.

A recent litigation involving two high profile companies, Oracle and SAP, reminds us to consider a few general rules before deploying a bot.

Rule #1: Don't be a Spammer

People, including judges, hate spam. If you use a bot to collect email addresses or other contact information and send unsolicited information, you are likely to anger someone enough to cause them to sue. Chances are you will lose the resulting case.

In one of the earliest web scraping cases, *America Online Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444 (E.D. Va. 1998), LCGM used a bot to collect names of AOL customers and sent spam to those customers. The court found that LCGM interfered with AOL's computer system by occupying its capacity and that sending spam may have injured AOL's business good will.

Rule #2: Think Twice Before Scraping Your Competitors

Many screen scraping cases involve scraping information from the website of a competitor on a competing site. This form of scraping almost always results in trouble, especially where the site has posted terms of use prohibiting commercial use of the site's content. Even data aggregators that ultimately direct traffic and sales to the originating sites have found themselves losing in court.

In *eBay v. Bidder's Edge*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000), Bidder's Edge used a bot to pull data from eBay's website in order to aggregate information across numerous online auction sites. The bot visited eBay's site about 100,000 times per day without authorization and in violation of eBay's stated policies. Damage was established in the form of lost server capacity.

However, in *Ticketmaster Corp. v. Tickets.com*, CV99-7654-HLH, 2000 U.S. Dist. LEXIS 12987 (C.D. Cal. Aug. 10, 2000), the court rejected the application of the *eBay* case to a case involving similar facts. Tickets.com used a bot to repeatedly access Ticketmaster's website to copy the factual information on the site regarding concert and event information. The court thought there was insufficient evidence of physical harm to the site's computers or obstruction of the website's basic functionality. While courts typically enforce a website's terms of use, the court declined to enjoin Tickets.com on the basis that there was no proof of agreement between Ticketmaster and Tickets.com merely from the posting of the terms alone.

In *Register.com v. Verio, Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000), Verio used bots to repeatedly copy the WHOIS database of contact information for domain name registrants from Register.com's website. Verio used that information to solicit registrants' interest in Verio's competitive services. Verio provided misleading information which potentially led registrants to believe that the solicitation came from a Register.com affiliate. The court found that Verio was bound by Register.com's website terms of use, even though Verio did not have to click to accept them. The terms stated that by submitting queries to the database the user was bound by the terms. Harm was shown by evidence that Verio's bots consumed as much as 2.3% of Register.com's system resources, potentially slowing the response times of the databases and even overloading them. The court also noted that "evidence of mere possessory interference" would be sufficient harm to support Register.com's claims.

In *Oyster Software, Inc. v. Forms Processing, Inc.*, C-00-0724-ICS, 2001 U.S. Dist. LEXIS 22520 (N.D. Cal. Dec. 6, 2001), Oyster complained that Forms Processing used a bot to copy the metatags on Oyster's site in order to redirect web user searches to its own site, where it sold directly competing products. The court held that the mere fact that the conduct was an unauthorized use of Oyster's computer system was sufficient for Oyster's claims to proceed to trial.

In *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001), Explorica deployed a bot to scrape 60,000 lines of data from EF's website to determine all its prices for global high school student tours in order to offer a competing service at lower prices. EF's server was accessed more than 30,000 times. The court held that EF's expenditure of substantial sums to assess the extent, if any, of the physical damage to their website caused by the intrusion was sufficient to support an injunction forbidding Explorica's scraping.

Most recently, Oracle sued SAP AG, No. 07-01658, (N.D. Cal. March 22, 2007), alleging that SAP used the login credentials of Oracle software customers to unleash a bot on Oracle's customer support website to download thousands of files and documents that SAP could then

use to provide lower-cost support services to Oracle software customers, without having to invest time and expense in developing such solutions themselves. This case is ongoing.

Rule #3: Maximize Benefit and Minimize Disruption to the Visited Site

Lawsuits typically result because the proprietor of a scraped site dislikes the way the scraped data is used. While spammers and direct competitors may simply be out of luck, there are other uses that companies may ignore, accept, tolerate, or even welcome.

Dynamically-generated content places more strain on web servers than static content.

If the bot you are thinking of using requires thousands of dynamically-generated results, performed every day in perpetuity, then the owner of the targeted site is going to notice and will not be amused.

Find a way to:

1. retrieve static content instead of dynamic content,
2. limit the total number of requests coming from the bot,
3. limit the amount of data retrieved in each request, or
4. space out the requests over longer time intervals.

Otherwise, you should consider asking permission from the visited sites.

Technically-savvy readers maybe thinking of ways to disguise the origin of the bot's requests. Bidder's Edge tried a rotating system of proxy services which disguised the origin of its bot's requests to eBay's site. This merely started a technological arms race in which eBay developed ever-more sophisticated means of detecting Bidder's Edge's requests while Bidder's Edge kept trying—and failing—to disguise the origin of the requests. Being sneaky also doesn't make you look good in court.

You may get away with it if:

1. your use for the data is not aimed at stealing or harassing a target site's customers,
2. you can find a minimally-intrusive means of collecting the data, and
3. you aren't constrained by the site's terms of use.

If so, you may find that sites will ignore, accept, or tolerate your bot and your use of the data.

To have a site welcome your bot, you need something more: a planned usage that benefits the site itself. While Bidder's Edge and Tickets.com actually drove more traffic to the sites they targeted, they didn't do enough to satisfy the plaintiffs who sued them. Some sites want to ensure that their advertising is viewed and so will object to any middle-man that directs customers directly to the products, services, or data they seek. Others are more practical and will accept such arrangements so long as an appropriate fee is paid.

This is not to say there is no reason to feel frustrated that companies are able to charge for otherwise freely available information. There's also an inherent line-drawing problem in encouraging individuals to visit one's site for free, but suing a company that visits 1,000 times per day. Would 500 times be too much? How about 150? You don't know when you are going to step across that subjective line.

Courts have not been terribly sympathetic to screen scraping, and so principled positions are typically going to give way to practical solutions.

Quick Updates

Court Rules That Maintaining Privacy in Business Relationships May Not be Sufficient to Protect Trade Secrets

Keeping your work private from the world is not sufficient to maintain it as a trade secret. On May 24, 2007, in *Incase Inc. v. Timex Corp.*, 488 F.3d 46 (1st Cir. 2007), the First Circuit Court of Appeals ruled that to protect a trade secret, affirmative steps must be taken to preserve its secrecy regarding a party against whom misappropriation is claimed.

The lawsuit arose from a business deal in which Timex hired product packaging designer and manufacturer Incase to design packages for Timex watches. The parties worked together to design a watch packaging for retail display that included a price flag for displaying the watch price. Timex ultimately purchased fewer of the units than initially agreed. In the meantime, the parties had begun work on a next generation packaging design including a removable price flag that was particularly important to Timex and that was more advanced than prior removable flags. Over the course of a year, the parties went back and forth with different designs for this new packaging until the design was nearly finished. Unbeknownst to Incase, however, Timex was also in discussions with Yuhig, a manufacturing company in the Philippines. Timex used Incase's packaging drawings and prototypes to produce a similar packaging with Yuhig, including the removable price flag. Timex ultimately purchased all of its packaging units from Yuhig rather than Incase.

In March 2001, Incase's vice president noticed the Timex watches displayed in a Target store in the Yuhig

packaging with the removable price flag design. Incase responded by suing Timex for trade secret misappropriation of the flag design, among other claims. The jury returned a verdict for Incase on all claims, but the district court overturned the jury's verdict as a matter of law on the trade secret issue. Both parties appealed, including an appeal from Incase on the trade secret judgment.

The appeal of the trade secret ruling focused on whether Incase took reasonable steps to preserve secrecy of the removable price flag design. Incase had not marked any documents "confidential," had not taken security precautions or required a non-disclosure agreement, and had not told Timex the design was a secret. Further, Incase's principal designer admitted that he did not believe the design to be a secret. Incase argued, however, that they had maintained secrecy by showing the designs only to Timex. Incase further pointed to the standard trade practices of secrecy in the watch packaging industry along with Timex's treatment of the designs as confidential when dealing with Yuhig.

The First Circuit found that there was no evidence to support Incase's arguments that reasonable steps were taken to preserve secrecy of the design. Though Incase's vice president testified that he had treated the designs as confidential, he admitted that this policy was never articulated to Timex. The court concluded that keeping the design secret from the public was insufficient to make it a trade secret since discretion is a normal feature of business relationships. Instead, affirmative steps should have been taken to protect a trade secret from Timex, the particular party against whom the misappropriation is claimed.

Federal Circuit Again Addresses Jurisdiction Over Declaratory Judgment Claims and Confirms That a Patentee May Still Escape Declaratory Claims by Dismissing Its Claims and Granting a Covenant Not to Sue

The Federal Circuit recently held that the Supreme Court's *MedImmune* decision did not alter a patentee's ability to avoid declaratory judgment claims by dismissing its claims and issuing a covenant not to sue. *Benitec Australia, Ltd. v. Nucleonics, Inc.*, 83 U.S.P.Q.2d 1449 (Fed. Cir. July 29, 2007).

The patentee, Benitec, sued Nucleonics for patent infringement for its development work relating to RNA-based disease therapy. Nucleonics later asserted declaratory counterclaims of invalidity and unenforceability. After the Supreme Court issued its decision in *Merck KGaA v. Integra Lifesciences I, Ltd.*, 545 U.S. 193 (2005), Benitec concluded that it no longer possessed viable infringement claims against Nucleonics and sought to dismiss its complaint, along with Nucleonics's declaratory counterclaims, without prejudice. The district court granted the dismissal.

Nucleonics challenged the dismissal on the grounds that Benitec's covenant not to sue failed to divest the court of jurisdiction and, although its past and current work relating to the human application of RNAi was exempt from claims of infringement pursuant to 35 U.S.C. § 271(e)(1), Nucleonics had taken steps to expand its business to animal RNAi products, which business it contended was not exempt under 35 U.S.C. § 271(e)(1). In particular, Nucleonics had entered into discussions with another party regarding providing animal RNAi products and executed a non-disclosure agreement, which was a precursor to "detailed technical discussions." Nucleonics also submitted an uncontroverted declaration that its work and research relating to animal RNAi products would "commence shortly." During the appellate proceedings, Benitec granted Nucleonics a covenant not to sue for "patent infringement for any activities and/or products occurring on or before the date of dismissal."

The Federal Circuit upheld the dismissal of the declaratory counterclaims and confirmed that the doctrine set forth in *Super Sack Manufacturing Corp. v. Chase Packaging Corp.*, 57 F.3d 1054 (Fed. Cir. 1995), and its progeny remains intact. Specifically, the Federal Circuit confirmed that a patentee's mid-suit grant of a covenant not to sue can divest a court of subject matter jurisdiction over declaratory judgment claims. It also noted that *Fort James Corp. v. Solo Cup Co.*, 412 F.3d 1340 (Fed. Cir. 2005), which held that a patentee's post-trial grant of a covenant not to sue failed to divest the court of jurisdiction, was an exception to the general rule and limited to a situation in which trial of the infringement issue has already occurred. The Federal Circuit also distinguished *SanDisk Corp. v. STMicroelectronics NV*, 480 F.3d 1372 (Fed. Cir. 2007), on the ground that the patentee in that case merely had made a statement regarding its intent not to sue, rather than a legally-binding promise.

As to Nucleonics's plans with respect to animal RNAi products, the Federal Circuit held that Nucleonics failed to demonstrate that it had engaged in any "use" of a patented invention, thus it had not engaged in any "present activity" that could give rise to a claim of infringement. Accordingly, despite its intent to commence work shortly, Nucleonics's plans to engage in potentially-infringing activity in the future failed to meet the "immediacy and reality requirement" of *MedImmune*. The Court further held that Nucleonics failed to carry its burden to show jurisdiction because it did not submit sufficient information to evaluate whether Nucleonics's future work would be potentially infringing or whether the exemption of section 271(e)(1) would apply to that work.

In closing, the Federal Circuit acknowledged Nucleonics's desire to remove concerns that it or potential investors might have concerning infringement of Benitec's patent, but concluded that Nucleonics failed to carry its burden of showing a dispute of "sufficient immediacy and reality."

Developments in Trademark Law Relating to Keyword Advertising

The extent to which trademarks can be used for keyword advertising was a hot topic in the summer of 2007. State regulation of keyword advertising emerged; one high profile lawsuit in this area fizzled just as another was being filed.

In June, amendments to the Utah state trademark statute became effective that established "a new type of mark, called an electronic registration mark, that may not be used to trigger advertising for a competitor." S.B. 236 Trademark Protection Act (2007). Several commentators have questioned whether Utah's new statute is constitutional. A legislative review note from Utah's own Office of Legislative Research and General Counsel, dated February 14, 2007, stated, "[T]his legislation has a high probability of being held to be unconstitutional." Internet commentators have also been blunt in stating that the law represents bad policy. In particular, the law's impact on comparative advertising, generally considered to be a social benefit, has been the target of many commentators' criticism. Since becoming effective on June 30, there has been no known enforcement of the law and no legal challenges have been reported as of the date of this writing. However, it does seem highly likely that sometime in the near future the policy underlying this law will be put to a test in court.

Separately, a high profile lawsuit against Google about whether current trademark law allows use of trademarked words as keywords was dismissed in early September via a settlement agreement, with Google reportedly neither making any payment nor altering its trademark policies. Headlines following the agreement characterized such lawsuits as a "sucker's bet."

At issue in the case was Google's "AdWords" program, which allows advertisers to pay to have their ads appear as "Sponsored Links" when users search for certain keywords, which can be generic or trademarked terms. This practice by search engines is commonly known as "keyword advertising." This case began in 2004, when American Blind & Wallpaper Factory objected that competitors' ads popped up as "Sponsored Links" when a user searched for "American Blind," one of its trademarks, in Google's search engine. ABWF sued Google, arguing that the "AdWords" program constituted trademark infringement. To prove trademark infringement, ABWF had to show that it has a valid and legally protectable mark, and that Google used the mark in commerce, "in connection with the sale, offering for sale, distribution, or advertising" of goods/services and in a way likely to confuse consumers.

Google filed a motion for summary judgment, which the court granted in part. The court granted summary judgment against ABWF as to some of its marks, dismissed ABWF's trademark dilution claims, held that use of trademarks in a keyword advertising context can constitute a "use in commerce," and found that there were issues of fact surrounding likelihood of confusion. *Google, Inc. v. American Blind & Wallpaper Factory, Inc.*, 2007 U.S. Dist. LEXIS 32450 (N.D. Cal. April 18, 2007).

Shortly before the settlement in the *Google v. ABWF* case was announced, American Airlines filed an action against Google based on keyword advertising using American Airlines trademarks. Thus, the development of this area of law is likely to continue in coming months.

Credit Card Companies Not Liable for Copyright Infringers' Acts

In the 1940s, Jehovah's Witnesses, tenaciously litigious in defense of free expression, generated a half-dozen Supreme Court decisions that came to define First Amendment rights in the Twentieth Century. With comparable persistence, erotic photo publisher Perfect 10 has fought a series of battles that may delineate the scope of secondary liability in the online kingdom. In July, Perfect 10 lost the third Ninth Circuit case this year in which it sought to make others responsible for direct copyright infringement and other wrongs committed by pornographic internet services. *Perfect 10 v. Visa International*, 2007 U.S. App. Lexis 15824 (July 3, 2007).

In the *Visa* case, a divided panel held that processing payments for infringing website services was too remote from the direct copyright infringements for Visa and the other credit card companies (collectively "Visa") to be held contributorily or vicariously liable.

The first of the Perfect 10 trilogy, *Perfect 10 v. CCBill*, 481 F.3d 751 (9th Cir. 2007), was brought against companies that provide web hosting and online credit card processing services to internet enterprises that directly infringed Perfect 10's copyrights. In March, the Ninth Circuit held that Perfect 10's state law claims were preempted by Section 230 of the Communications Decency Act, determined that Perfect 10's Digital Millennium Copyright Act infringement notices were insufficient to require the defendants to take down allegedly infringing matter, and remanded for further consideration the defendants' entitlement to the DMCA's safe harbors. In May, another Ninth Circuit panel rejected most of the theories whereby Perfect 10 sought to hold Google liable for providing visual search engine services that facilitated locating and

accessing infringing sites. *Perfect 10 v. Amazon*, 487 F.3d 701 (9th Cir. 2007).

In *Perfect 10 v. Visa*, the district court dismissed for failure to state a claim, holding *inter alia* that Visa was not contributorily or vicariously liable under copyright law. The same panel of the Ninth Circuit as in *CCBill* affirmed.

For contributory infringement, the defendant must (1) have knowledge of an underlying direct infringement, and (2) materially contribute to it. Reviewing *de novo*, Circuit Judges Smith and Reinhardt held that Visa's activities did not materially contribute to infringement because facilitating payment bears "no direct connection to [the] infringement."

The majority emphasized that the underlying infringements — reproduction, alteration, display and distribution of Perfect 10's images — could occur regardless of whether Visa provided payment services.

In *Perfect 10 v. Amazon*, the Ninth Circuit held Google's search engine materially contributed to infringement because it assisted in locating and accessing infringing images by providing links to them. In addition, the music file-sharing services in Napster and Grokster were held contributorily liable because they allowed users to locate and obtain infringing material. Distinguishing these cases, the *Visa* majority argued that Visa's services do not cause the infringing activities, and that making it easier to profit from infringement is not essential to the conduct of infringement.

Amazon instructed that "Google could be held contributorily liable if it had knowledge that infringing Perfect 10 images were available using its search engine, could take simple measures to prevent further damage to Perfect 10's copyrighted works, and failed to take such steps." Dissenting Judge Kozinski argued that Visa's acts were equivalent to those in *Amazon*. The majority, however, held that payment systems and search engines are not equivalent because creating a financial incentive for infringement involves "an additional step in the causal chain" beyond facilitating connection with an infringing site.

The dissent responded that the credit card payment system is, as a practical matter, essential, and that in any event the test for "materially contributing" is merely whether the activity "substantially assists" infringement. Kozinksi also maintained that there was no additional step between Visa's activity and the direct infringement because payment is integral to one of the exclusive rights of copyright holders, "plaintiff's right of distribution 'by sale.' 17 U.S.C. section 106(3)." "It's not possible to distribute by sale without receiving compensation," Kozinski argued, "so payment is in fact part of the infringement process."

The majority noted that under the dissent's reasoning, a utility company that provides electricity to the direct infringer would be held to have materially contributed to the infringement. After all, if a power company is given notice of an alleged infringement, it can take "simple measures to prevent further damage to ... copyrighted works," namely, turning off the electricity.

A labyrinth of troubling issues concerning the "knowledge" element of contributory infringement would have to be threaded through if a broader class of enterprises is deemed to be materially contributing to infringing activity. For example, what if the alleged direct infringer has not created a counterfeit of the original work, but a work alleged to be "substantially similar"? What if fair use or protectability under copyright law poses significant issues?

By Perfect 10's logic, when a copyright holder puts a supporting player on notice for a claim of infringement, that entity must terminate services to the alleged direct infringer or investigate and make a judgment about whether the claim appears meritorious. But what kind of investigation is required? And by what standard should a credit card company or utility be deemed to "know" that the accused is an infringer? Is it enough to defeat such knowledge that the alleged direct infringer makes a non-frivolous argument of fair use?

Existing case law does not offer clear answers to these questions. But Congress, by providing safe harbors under the DMCA and immunity against various state law claims under the Communications Decency Act, powerfully signaled its policy determination that copyright holders must focus their policing efforts on the infringers themselves.

For vicarious liability, the defendant must have (1) the right and ability to supervise and control an underlying direct infringement from which it (2) obtains a direct financial benefit. Perfect 10 maintained that Visa had the right and ability to control infringement because the payment system allows the infringements to operate on a larger scale than they otherwise would. But, the majority held, that was insufficient. The dissent responded that Visa did have the right and ability to control infringement because its agreement with the charged websites reserved the right to require them to behave lawfully as a condition for obtaining Visa's payment services.

The last judicial word has not been uttered on *Perfect 10 v. Visa*. Leaning heavily on Judge Kozinski's vigorous dissent, Perfect 10 (supported by the usual suspects, the Motion Picture Association of America and the Recording Industry Association of America) has petitioned for rehearing and rehearing en banc. As of this writing, the petition is pending.

Fenwick

FENWICK & WEST LLP

Fenwick & West's Intellectual Property Group offers comprehensive, integrated advice regarding all aspects of the protection and exploitation of intellectual property. From providing legal defense in precedent-setting user interface copyright lawsuits to prosecuting software patents and from crafting user distribution arrangements on behalf of high-technology companies to implementing penetrating intellectual property audits, our attorneys' technical skills enable the Firm to render sophisticated legal advice.

Offices

801 California Street
Mountain View, CA 94041
Tel: 650.988.8500
Fax: 650.938.5200

555 California Street, 12th floor
San Francisco, CA 94104
Tel: 415.875.2300
Fax: 415.281.1350

www.fenwick.com

We appreciate your feedback!

If you have questions, comments, or suggestions for the editors of the IPB, you can e-mail them to IPB@fenwick.com.

For subscription requests and address changes, please e-mail IPB@fenwick.com.