Proskauer

New Media, Technology and the Law

Spring 2010

Edited by **Jeffrey D. Neuburger**

COPYRIGHT

Scope of Protection

Unauthorized Sharing of Copyrighted Music Files on P2P File-Sharing Network Not Protected by Fair Use Defense

A party who made copies of music recordings and shared them with other parties on a peer-to-peer file-sharing network is not protected by the defense of fair use, a district court ruled. The court concluded that the party's fair use defense could not be presented to the jury because the party had failed to allege any disputed facts that pertained to the issue of fair use, and on the undisputed facts, no reasonable jury could find in his favor on the issue. The court rejected the party's argument that the jury was entitled to broadly consider the party's defense that any non-commercial use is presumptively fair and that the jury was entitled to consider its “innate sense of fairness” in evaluating whether the party's use was fair.

Sony BMG Music Entertainment v. Tenenbaum, 2009 U.S. Dist. LEXIS 112845 (D. Mass. Dec. 7, 2009) Download PDF

Editor’s Note: As the court relates, this opinion memorializes the decision announced from the bench on the eve of the trial on the merits in July 2009, which resulted in a $675,000 infringement verdict against the defendant. The court's opinion is of interest for its suggestion that the fair use defense might be available for some instances of sharing music files, particularly during a prior period when the law pertaining to such sharing was less clear.

Floor Plans in Online Database Not Protectable under Copyright Law

Copying of floor plans that were collected from third parties and compiled into an online database is not actionable under copyright law, a district court ruled. The court ruled that the entire online database that contained content in addition to the floor plans was the result of independent selection, coordination and arrangement, and, therefore, was a copyrightable compilation. But the court further ruled that the floor plans themselves, which had been originally provided by the homebuilders and developers to the public, were uncopyrightable facts. The court also found that numeric indicators that were also copied by the defendant were “only useful internally” in the online database and were therefore not copyrightable original expression upon which a copyright infringement claim could be based. The court refused to dismiss the plaintiff's breach of contract claims, based upon the copying, reproduction and display of the floor plans without the plaintiff's consent, finding that those claims were not preempted by the Copyright Act.

Salestraq America, LLC v. Zyskowski, 2010 U.S. Dist. LEXIS 3384 (D. Nev. Jan. 14, 2010) Download PDF

Digital Millennium Copyright Act

Manufacturer of Device Containing DVD Player Has Standing to Assert Violations of DMCA Anticircumvention Provisions

The manufacturer of a device containing a DVD player that implements DVD copy protection technology has standing to bring an action against a party who allegedly disabled the copy protection technology on such devices before selling them in online auctions, a district court ruled. The court rejected the argument that the manufacturer did not have constitutional standing, because the manufacturer sufficiently alleged that the sale of the altered devices could reasonably be expected to deprive it of the opportunity to profit from the sale of unaltered devices. The court also concluded that the manufacturer was a "person injured" within the meaning of the DMCA anticircumvention provisions because the manufacturer is a "party who controls the technological measures that protect copyrighted works."

Bose BV v. Zavala, 2010 U.S. Dist. LEXIS 2719 (D. Mass. Jan. 14, 2010)

No Bad Faith in Filing Takedown Notice Where Resolution of Intellectual Property Rights Underlying DMCA Claim Involved Complex and Novel Legal Issues

A party who filed a takedown notice under the Digital Millennium Copyright Act seeking removal of a Web site in which he claimed copyright ownership did not act in bad faith where the resolution of the intellectual property rights underlying his claim involved complex and novel issues, a district court ruled. Following a bench trial, the court ruled adversely to the party's claim of copyright ownership in the disputed Web site, as well as his claim to other intellectual property assets of a business entity in which he was formerly a principal. But the court declined to find that the party's takedown notice was filed in bad faith under DMCA § 512(c)(3). The court noted that the good faith belief standard in the DMCA takedown provision is a subjective good faith standard and a party is not liable under the DMCA for making an unknowing mistake, even if the mistake was objectively unreasonable. There was no evidence to suggest, the court found, that the party filing the notice acted without subjective good faith in filing the takedown notice.

Third Education Group, Inc. v. Phelps, 2009 U.S. Dist. LEXIS 116930 (E.D. Wisc. Nov. 25, 2009) Download PDF

Operator of BitTorrent P2P File-Sharing Network Induced Copyright Infringement and Is Ineligible for DMCA Safe Harbors

The operator of a file-sharing network that utilized the BitTorrent file-sharing technology is secondarily liable for inducing copyright infringement by users of the network, a district court ruled. The court noted the unrebutted evidence proffered by the motion picture company plaintiffs establishing massive sharing of unauthorized copies of their copyrighted works on the network. The court found, among other things, that the plaintiffs showed that the defendant operator disseminated messages to users that were designed to stimulate them to commit infringement, and that the defendant and others under his control provided assistance to users in downloading and locating infringing files. The defendant also implemented technical measures aimed at promoting copyright infringement, such as the use of “spider” programs to locate and obtain copies of infringing files on other file-sharing networks, and profited from the infringement by selling advertising space on his Web site based upon the infringing content that was made available. The court rejected the defendant's claim to the safe harbors under DMCA 512(c) on the ground that the proof of the defendant's inducement of the infringing conduct established that the operator had reason to know of the infringing conduct on the part of users of the network.

Columbia Pictures Industries, Inc. v. Fung, 2009 U.S. Dist. LEXIS 122661 (C.D. Cal. Dec. 21, 2009) Download PDF

Damages

Limited Damages Available under DMCA 512(f) for Wrongful Takedown Notice

Although DMCA 512(f) allows an award of “any damages” for wrongful removal of alleged infringing material as a result of misrepresentations to a service provider, such damages “must be proximately caused by the misrepresentation to the service provider and the service provider's reliance on the misrepresentation,” a district court ruled. The court rejected the argument that the plaintiff was required to show “substantial economic damages,” however, pointing to the “any damages” language and the deterrent purpose of the statute. The court also concluded that an award of attorney fees under DMCA 512(f) is limited to fees incurred in responding to the removal of the material prior to institution of suit, while attorney fees for bringing an action pursuant to DMCA 512(f) may be awarded pursuant to Section 505 of the Copyright Act.

Lenz v. Universal Music Corp., 2010 U.S. Dist. LEXIS 16899 (N.D. Cal. Feb. 26, 2010) Download PDF

Editor's Note: This case, often referred to as the "dancing baby" case, is best known for an earlier district court ruling finding an implied duty on the part of content owners preparing a takedown notice to "consider" whether the unauthorized use of its content is protected by the fair use doctrine. The August 2008 ruling is discussed on the Proskauer New Media and Technology Law blog.

Actual Damages for Copyright Infringement of Software Code Supported by Monetary Value of Work by Contributors to Open Source Project

A claim for actual damages for infringement of open source software code is not precluded because the code was distributed without charge, a district court ruled. The court denied the defendant's motion for summary judgment on the issue of actual damages, finding that a monetary damages figure could be established by evidence in the record attributing a monetary value to the actual work performed by contributors to the open source project that produced the software code.

Jacobsen v. Katzer, 2009 U.S. Dist. LEXIS 115204 (N.D. Cal. Dec. 10, 2009) Download PDF

Editor's Note The case is most significant for the August 2008 ruling by the U.S. Court of Appeals for the Federal Circuit that rights in open source software code can be enforced under the Copyright Act. In the current ruling, the district court noted that Jacobsen, the manager of the open source project that produced the code in question, and the assignee of the related copyright rights, conceded that he was not entitled to statutory copyright damages. The district court's opinion, including its rulings on several other issues, is discussed further on the Proskauer New Media and Technology Law blog, as is the announcement on February 17 of the settlement of the litigation.

College Student's Innocent Infringer Defense for Copying and Distributing Phonorecords on P2P Network Foreclosed by Copyright Notices

A college student found liable for copyright infringement for making digital copies of copyrighted phonorecords and sharing them on a P2P file-sharing network is not entitled to the mitigation of statutory damages under Copyright Act § 504(c)(2) for innocent infringement, the U.S. Court of Appeals for the Fifth Circuit ruled. The court noted that the innocent infringer defense is limited by Copyright Act § 402(d), which provides that "no weight" shall be given to the interposition of the innocent infringer defense where a notice of copyright appears on the phonorecords in question. The appeals court noted that the lower court had found that the college student had access to the phonorecords containing the copyright notices. The college student's lack of legal sophistication or intent to infringe, the appeals court found, were irrelevant in the context of the limitation in § 402(d).

Maverick Recording Co. v. Harper, 2010 U.S. App. LEXIS 3912 (5th Cir. Feb. 25, 2010) Download PDF

Near $2 Million Copyright Damages Verdict against Noncommercial File-Sharing Defendant Remitted as "Gross Injustice"

A $1,920,000 jury award of copyright damages against a "noncommercial individual" for distributing 24 copyrighted songs on a file-sharing network is a "gross injustice" that warrants remitting the verdict to three times the minimum statutory damages of $750 per song, or $2,250 per song ($54,000), a district court ruled. The court found that an award of three times the minimum statutory damages figure per work was justified in light of the defendant's willful conduct and was consistent with the practice of trebling damages under other statutory damages schemes, including the Digital Millennium Copyright Act and other federal laws. The resulting $54,000 damages amount is "significant and harsh," the court concluded, and reflects the "maximum amount a jury could reasonably award to both compensate Plaintiffs and address the deterrence aspect of the Copyright Act."

Capitol Records Inc. v. Thomas-Rasset, 2010 U.S. Dist. LEXIS 5049 (D. Minn. Jan. 22, 2010) Download PDF

Editor's Note: The verdict that was remitted by the court was delivered in the second trial in this case. After the second trial and following negotiations between the parties that reportedly included an offer on the part of the plaintiffs to accept $25,000 in damages, and a refusal of that offer by the defendant, the court's remittitur was refused. The court then announced that a third trial, on the issue of damages only, would be scheduled.

DEFAMATION

Web Site Addition of Hyperlinks to a Previously Posted Online Article Does Not Restart Defamation Statute of Limitations

The addition of hyperlinks to an allegedly defamatory online article does not restart the statute of limitations for defamation, a district court ruled. Applying Kentucky law, the court concluded that Kentucky would apply the single publication rule to online articles, and that under that rule, only a republication of an online article could restart the statute of limitations. The court further concluded that the addition of hyperlinks did not constitute a republication because their addition merely drew the existence of the article to a new audience, it did not present the defamatory contents of the article to that audience. Referring to the legislative intent to limit the time period within which defamation claims could be brought, the court commented: "Methods of access to portions of [a] website can change on a regular basis and links to previous posts on a website are constantly added and taken away from sites. Therefore to find that a new link to an unchanged article posted long ago on a website republishes that article would result in a continual retriggering of the limitations period."

Salyer v. The Southern Poverty Law Center, Inc., 2009 U.S. Dist. LEXIS 113511 (W.D. Ky. Dec. 4, 2009) Download PDF

RIGHT OF PUBLICITY

Depiction of Student Athlete in Videogame Deemed Actionable under California Right of Publicity Statute

The inclusion of a character in a videogame that corresponded to a student athlete is actionable under the California right of publicity statute, a district court held. The court rejected the videogame producer's defense that the use of the character was protected by the First Amendment. The court found that the videogame character was not sufficiently transformative because it corresponded to the athlete's sport, collegiate team, playing position, jersey number, height, weight and home state, and was depicted in the same setting, collegiate sports, in which the athlete functioned during his sports career. The court also rejected several other defenses, including the argument that the inclusion of the characters was protected by the First Amendment interest in reporting athletic performances.

Keller v. Electronic Arts, Inc., 2010 U.S. Dist. LEXIS 10719 (N.D. Cal. Feb. 8, 2010) Download PDF

California Single Publication Rule Applies to Web Site Right of Publicity, Lanham Act Claims

The California single publication rule bars an individual's common law and California statutory right of publicity and Lanham Act false endorsement claims for the sale of merchandise on a Web site, a district court ruled. The court found that the individual's claims were based upon material that had been on the defendant's Web site since 2000, outside the statute of limitations period for either the right of publicity claims or Lanham Act claims. The court rejected the plaintiff's argument that the single publication rule did not apply because the Web site seller was engaged in a series of ongoing sales for commercial gain, resulting in a re-starting of the limitations period for each sale. The court commented that acceptance of the plaintiff's argument on this point would mean that the statute of limitations would never run while the Web site remained in existence with the subject items for sale, and that this was a result that this would be “the exact result the single publication rule seeks to avoid.”

Yeager v. Bowlin, 2010 U.S. Dist. LEXIS 718 (E.D. Cal. Jan. 6, 2010) Download PDF

COMMUNICATIONS DECENCY ACT

Addition of Introduction and Forwarding of Defamatory E-Mail Protected from Liability under CDA Section 230

The recipient of a defamatory e-mail who forwarded it to other parties with a brief introduction is protected from liability for defamation by Section 230 of the Communications Decency Act, a panel of the California Court of Appeal ruled. The appeals court examined the ruling of the Ninth Circuit in Fair Housing Council of San Fernando Valley v. Roommates.Com (9th Cir. 2008), and concluded that the proper test for whether the addition of material to an defamatory e-mail renders the forwarder an "information content provider" within the meaning of Section 230 is whether the additional material is a "material contribution" to the defamation contained in the message. The court concluded that the forwarder's statements in the introduction, which suggested that the further recipients should read it and that "the truth will come out in the end," did not materially contribute to the alleged defamation in the e-mail.

Phan v. Pham, 2010 Cal. App. LEXIS 239 (Cal. Ct. App. 4th Dist. Feb. 25, 2010)

Advertiser Protection under CDA Section 230 for User-Generated Online Contest Submissions Held an Issue for Jury

Material issues of fact concerning an advertiser's role in the creation of user-generated videos submitted in an online contest preclude a grant of summary judgment on the issuer's defense under Section 230 of the Communications Decency Act, a district court ruled. The case involved a lawsuit brought by a franchisor against a competitive franchisor alleging false and deceptive advertising, among other things, and claiming that the competitive franchisor was responsible for unfair comparisons between the products of the two franchisors that were made in the user-generated videos submitted during the online contest. The court concluded that it was unclear at the pre-trial stage of litigation whether the competitive franchisor went beyond the traditional role of a publisher with respect to the contest videos and actively participated in creating or developing the third-party content; the question of whether the competitive franchisor was an "information content provider" not entitled to the protection of Section 230 was a question for the jury.

Doctor's Associates v. QIP Holder LLC, 2010 U.S. Dist. LEXIS 14687 (D. Conn. Feb. 19, 2010). Download PDF

Editor's Note: Shortly after the ruling was issued, the parties notified the court that the case had been settled. This case is discussed on the Proskauer New Media and Technology Law blog.

Complaint Containing Bare Allegations That Consumer Complaint Web Site Is an "Information Content Provider" Properly Dismissed under CDA Section 230

A complaint containing bare allegations that a consumer complaint Web site solicited complaints, contacted consumers to ask questions and assist in drafting or revising complaints, and steered the complaints to categories designed to attract the attention of class action lawyers, among other things, was properly dismissed pursuant to Section 230 of the Communications Decency Act, the U.S. Court of Appeals for the Fourth Circuit ruled. The court concluded that the allegations concerning assistance with revising and redrafting complaints failed to show anything more than conduct that a Web site operator engages in as "part of its traditional editorial function." The court also noted that there is "nothing illegal" about developing content related to class actions lawsuits and that such lawsuits are specifically provided for in the federal rules.

Nemet Chevrolet, LTD v. Consumeraffairs.com, Inc., 591 F.3d 250 (4th Cir. Dec. 29, 2009) Download PDF

Allegations That Employee of Web Site Operator Promised to Remove Defamatory Content Preclude Summary Judgment on Promissory Estoppel Claim

Allegations by the plaintiff in a defamation action that a Web site operator's employee said she would "take care" of having false and defamatory profiles removed from the site were sufficient to create an issue of fact precluding summary judgment on the plaintiff's promissory estoppel claim, the district court ruled. The court noted that according to the plaintiff, she had tried for months to have the defamatory profiles removed, and the employee said she would "take care" of having them removed after having been contacted by a news reporter interested in doing a story on the plaintiff's situation, but failed to do so. The court concluded that there was a "reasonable and plausible inference" that the plaintiff relied upon the employee's promise to her detriment when she contacted the reporter and headed off the news story, thereby delaying the removal of the defamatory profiles.

Barnes v. Yahoo!, Inc., 2009 U.S. Dist. LEXIS 116274 (D. Ore. Dec. 8, 2009) Download PDF

Editor's Note: The matter was remanded to the district court as a result of the appellate court ruling in Barnes v. Yahoo!, Inc., 570 F. 3d 1096 (9th Cir. 2009), holding that the plaintiff's promissory estoppel claim was not precluded by Section 230 of the Communications Decency Act. See further discussion of the district court opinion on the Proskauer New Media and Technology Law blog.

Fed. R. Civ. P. 65 Precludes Post-Judgment Injunction Requiring Web Site to Remove User's Defamatory Post

The requirements of Fed. R. Civ. P. 65 preclude the enforcement of an injunction requiring the removal of posts found to be defamatory against a Web site operator that was not a party to the defamation litigation in which the judgment including the injunction was issued, a district court ruled. The court noted that the federal rule permits the enforcement of a judgment against a non-party only if there is a showing that the non-party acted in concert or is legally identified with the enjoined party. The court rejected the argument that the acting in concert requirement could be established by the Web site terms of service to which the user assented, which included a provision stating that the Web site would not remove posted material even at the request of the user. The court noted the provision requiring users to post only "truthful and accurate" statements on the site, and found that the record was "devoid of any evidence" that the Web site operator intended to "protect defamers and aid them in circumventing court orders."

Blockowicz v. Williams, 2009 U.S. Dist. LEXIS 118599 (N.D. Ill. Dec. 21, 2009) Download PDF

Editor's Note: This case is discussed on the Proskauer New Media and Technology Law blog. Note that the court noted, but did not rely upon, Section 230 of the Communications Decency Act.

Failure to Allege That Defendants Were Authors of Defamatory Posts Merits Dismissal under CDA Section 230

An action for defamation based upon comments on a Web site allegedly operated by the defendants was properly dismissed pursuant to Section 230 of the Communications Decency Act, where the plaintiff failed to allege that the defendants were the authors of any of the defamatory statements. The court noted that the plaintiff's complaint alleged only that the defendants “choose and administer content” that appeared on the Web site, and that they engaged in a calculated effort to encourage, keep and promote “bad” content on the site. The court found that these allegations were insufficient to establish a claim that the defendants were “information content providers” with respect to the allegedly defamatory posts.

Shiamili v. Ardor Realty Corp., 2009 N.Y. App. Div. LEXIS 9210 (Sup. Ct. App. Div. 1st Dept. Dec. 17, 2009) Download PDF

ONLINE CONTRACTS

Forum Selection Clause Specifying State Court Venue Operated as Waiver of Federal Forum for Claims under ECPA

A forum selection clause in an agreement for online services that required claims to be brought in the “courts of Virginia” operated as a waiver of a user’s right to litigate claims under the Electronic Communications Privacy Act in a federal forum, a district court ruled. The court noted that the U.S. Court of Appeals for the Ninth Circuit had previously ruled that the phrase “courts of Virginia” meant the state courts of Virginia and excluded a federal forum. Federal and state courts have concurrent jurisdiction over claims under the ECPA, the district court ruled on remand, therefore the forum selection clause could operate to require adjudication of those claims in state court. The forum selection clause operated as a waiver of the plaintiff’s right to adjudicate the ECPA claims in a federal forum, the court further ruled, because the plain meaning of the language in the forum selection clause specifying jurisdiction over “any claims or disputes” was sufficiently broad to encompass both federal and state claims.

Doe I v. AOL, LLC, 2010 U.S. Dist. LEXIS 14639 (N.D. Cal. Feb. 1, 2010) Download PDF

Editor's Note: The underlying lawsuit raises various state and federal privacy and related claims arising from the public release of anonymized data concerning the search results of 650,000 users of the AOL search engine in 2006. Note that under the Ninth Circuit's prior ruling in the case, the forum selection clause is enforceable only as to plaintiffs who are not residents of California.

Forum Selection Clause in Google Adwords Agreement Applies to Claims against Google for Prior Conduct

The scope of the forum selection clause in the agreement applicable to the Google Adwords program extends to a plaintiff's dispute with Google over conduct predating the execution of the Adwords agreement, a district court ruled. The court relied upon language in the agreement providing that the clause applies to "all claims arising out of or relating to this Agreement or the Google Programs." The court concluded that the plaintiff's trademark infringement claims against Google for its sale of the plaintiff's trademark to other advertisers fell within the plain language of the forum selection clause, and that there were no legal reason why the clause was limited to claims depending upon the contractual relationship between the parties or to claims arising subsequent to the execution of the agreement.

Flowbee International Inc. v. Google, Inc. (S.D. Tex. Feb. 8, 2010) Download PDF

Editor's Note: Based on this court's decision, it may be advisable to be very specific about the scope and applicability of a forum selection clause to disputes between the parties that preexist the effective date of the contract.

Online Clickwrap Forum Selection Clause Enforceable Despite User's Claim of Accidental or Involuntary "Click"

A forum selection clause in an online clickwrap agreement covering financial information services is enforceable despite the user's claim that he may have accidentally or involuntarily clicked the boxes signifying assent to the agreement, a district court ruled. The court concluded that the plaintiff's contention that his “click” was inadvertent was not credible, and that the evidence established that users could not complete the defendant's required registration process without clicking both an “I agree” box adjacent to the terms and conditions and a “complete registration” box. The court also rejected the argument that the defendant should have used computer technology that requires users to scroll down through all of the terms in an online agreement, finding that imposing “such a per se legal requirement on internet companies in order to enforce a contract would be the equivalent of requiring a party to a paper contract to ensure that the opposing contractual party flipped through all the pages before signing it.”

Scherillo v. Dun & Bradstreet, Inc., 2010 U.S. Dist. LEXIS 13465 (E.D.N.Y. Feb. 17, 2010) Download PDF

Online Clickwrap Agreement Unenforceable Where Customer Warned Company That Non-Executives Had No Contractual Authority

A forum selection clause in an online clickwrap agreement is not enforceable against a customer that warned the Web site owner that it would not assent to such agreements, and that the customer's employees who accessed the site were not authorized to enter agreements on the customer's behalf, a district court ruled. The court noted that the customer and the Web site owner had a preexisting dispute, but the customer's employees still accessed the the owner's Web site to utilize previously contracted-for services. The court further noted that in order to access the site, the employees were required to click “I agree” to the terms presented on the site. The court held that the employees did not have legal authority to bind the company, and that under the circumstances presented it was unreasonable for the Web site owner to believe that they had such authorization.

National Auto Lenders Inc. v. SysLOCATE Inc., 2010 U.S. Dist. LEXIS (S.D. Fla. Feb. 10, 2010) Download PDF

Editor’s Note: How can an ASP software provider assure that the corporate user of its system has the authority to bind the company? In certain situations, a side letter to that effect may be appropriate.

Arbitration Clause in Electronic Employment Agreement Unenforceable Where Evidence of Execution and Assent to Arbitration Were Lacking

An arbitration clause in an electronic employment agreement cannot be enforced where the employer failed to show by a preponderance of the evidence that the employee electronically executed the agreement, a California appeals court ruled. The court found that the evidence before the lower court indicated that the form in question had been partially filled out at the time it was presented to the employee, and the system through which the document was provided allowed the document to be edited and electronically signed by individuals other than the employee. Absent affirmative evidence that the employee herself electronically signed the agreement, the court concluded, it could not find that the purported electronic signature on the document was attributable to the employee under the California Civil Code provisions governing electronic transactions. The court also found that even if the employee had signed the agreement, she was not sufficiently alerted to the fact that it contained an arbitration provision.

Adams v. Superior Court, 2010 Cal. App. Unpub. LEXIS 1236 (Cal. Ct. App. 4th Dist. Feb. 22, 2010) Download PDF

Clickwrap Agreement Enforceable Between Commercial Parties, Where Contract Formation Process Was "Consistent with Industry Standards"

A clickwrap agreement between a retail Web site operator and a commercial party was enforceable because, among other things, the online contract formation process that led to the agreement was "consistent with industry standards" and thus could not be said to be substantively unconscionable, a district court ruled. The court also rejected the plaintiff's argument that its employee did not know that he was entering into a contract and that he was not authorized to do so, noting that the employee was over 18, the employee admitted checking the "I accept … the terms of service" box that was adjacent to a clickable icon at which the terms could be accessed, and that it was undisputed that the CEO of the plaintiff company reviewed the terms of service and that the company paid for the services that were provided under the contract. In rejecting the substantive unfairness argument, the court noted that the contract formation process on the Web site of the plaintiff who was seeking to avoid the enforcement of the clickwrap agreement was similar to that of the Web site operator, and the terms on the plaintiff's own Web site appeared to be similar to those in the agreement that it was challenging.

Appliance Zone, LLC v. Nextag, Inc., 2009 U.S. Dist. LEXIS 120049 (S.D. Ind. Dec. 22, 2009) Download PDF

Exculpatory Clause in Commercial Contract for Internet Services Not Unconscionable

A lawsuit by a customer seeking damages from an Internet Service Provider (ISP) for termination of the customer's Internet connectivity was properly dismissed pursuant to the terms of the exculpatory clause in the ISP's service agreement, the U.S. Court of Appeals for the Third Circuit ruled. The ISP notified the customer that it was terminating service for violations of its acceptable use policy, based upon numerous complaints received concerning the content of e-mails sent from IP addresses associated with the customer. The appeals court concluded that the exculpatory clause was neither adverse to the public interest nor unconscionable under New Jersey law. The court noted, among other things, that the customer was a commercial entity experienced with Internet service agreements, and that the term was “prominently presented” in the agreement and was not unreasonably oppressive.

Asch Webhosting, Inc. v. Adelphia Business Solutions Investment, LLC, No. 09-2296 (3d Cir. Jan. 25, 2010) (unpublished) Download PDF

Clickwrap Form of Online Agreement Not Required for Contract Formation

A click on a button marked “I agree” is not necessary to effectively manifest assent to online contract terms, a Missouri appeals court ruled. The court rejected a consumer's argument that a forum selection clause was unenforceable because she had not read and had not assented to the Web site terms and conditions in which it was contained. The court noted that at the point where the consumer submitted a request for information provided by the Web site, she was presented with a hyperlink to the terms and conditions which was labeled with the following notice: “By submitting you agree to the Terms of Use.” The court rejected the principle that clickwrap agreements are better for proving assent, commenting that there is “no fundamental reason” to require manifestation of assent by a click on the statement “I agree.”

Major v. McCallister, 302 S.W.3d 227 (Mo. Ct. App. Dec. 23, 2009) Download PDF

Arbitration Clause in Computer Purchase Contract Unenforceable Where Consumer's Right to Reject Additional Terms Was Not Clearly Explained

A computer seller's terms and conditions included with a mail order purchase were not enforceable where the consumer purchaser's right to reject the contract by returning the goods was not clearly explained, the Supreme Court of Rhode Island ruled. The court noted that although the terms and conditions document containing the arbitration clause included an “express disclaimer” informing the purchaser of the right to return the goods, the disclaimer was located in a separate provision removed from the introductory contractual language in the agreement, and the language of the disclaimer was confusing. Further, the court found the construction of the terms and conditions required the consumer to construe contractual language in order to infer the right to return the goods. Thus, the court concluded, it was not “reasonably apparent” to purchasers that they had a right to reject the contract provisions by returning the goods.

Defontes v. Dell, 2009 R.I. LEXIS 142 (R.I. Dec. 14, 2009)

Editor’s Note This ruling is more fully discussed on the Proskauer New Media and Technology Law blog.

COMPUTER FRAUD AND ABUSE ACT

Employee Access to Computer Network in Furtherance of Criminal Fraud “Exceeds Authorized Access” under CFAA

An employee who accessed financial data on her employer's computer network in violation of official policy in order to perpetrate a criminal scheme exceeded her authorized access to the network within the meaning of the Computer Fraud and Abuse Act, the U.S. Court of Appeals for the Fifth Circuit ruled. The court upheld the employee's conviction under 18 U.S.C. § 1030(a)(2) for exceeding authorized access to financial information, for copying customer account information and furnishing it to confederates who used it to incur fraudulent charges. The court concluded that exceeding authorized access under the CFAA encompasses limits placed on the use of information obtained, “at least when the user knows or reasonably should know that he or she is not authorized to access a computer and information obtainable from that access [is used] in furtherance of or to perpetrate a crime.”

United States v. John, 2010 U.S. App. LEXIS 2742 (5th Cir. Feb. 9, 2010) Download PDF

Editor's Note: The court also noted, but distinguished, the ruling in LVRC Holdings LLC v. Brekka, (9th Cir. 2009), in which the Ninth Circuit in a civil action under the CFAA held that exceeding authorized access does not encompass misuse of data.

Rule of Lenity Limits Criminal Prosecution under Computer Fraud and Abuse Act for Acts of Employee Disloyalty

The rule of lenity limits prosecution of an allegedly disloyal former employee on the theory that his access to his employer's computer network was "without authorization" or "exceed[ed] authorized access" within the meaning of the Computer Fraud and Abuse Act, a district court ruled. The indictment alleged that the former employee was criminally liable for the acts of other employees who accessed the employer's computer network in order to copy confidential and proprietary information in order to utilize it in a competitive enterprise. The court reversed an earlier ruling sustaining the indictment, finding that the subsequent ruling by the Ninth Circuit in LVRC v. Brekka, 581 F.3d 1127 (9th Cir. 2009), rejected the theory that an employee's authority to access an employer's computer network was terminated by virtue of an act of disloyalty to the employer. The court held that under the ruling in LVRC v. Brekka, an employee's intent in access the employer's computer network is irrelevant in determining whether an employee's access is authorized under the CFAA.

United States v. Nosal, 2010 U.S. Dist. LEXIS 24359(N.D. Cal. Jan. 6, 2009) Download PDF

Editor's Note: This opinion is discussed in the Proskauer New Media and Technology Law blog.

No Cause of Action under CFAA for Unwanted Text Messages

Unwanted text messages sent to a subscriber's cellular phone do not give rise to a cause of action under the Computer Fraud and Abuse Act, a district court ruled. The court rejected the plaintiff's claims that the unwanted messages resulted in the unauthorized obtaining of information from her cell phone, finding that there was “no plausible basis” on which it could conclude that the sender of a text message necessarily obtains information from the receiving cell phone. The court rejected the plaintiff's argument that communicating with a cell phone via text message was analogous to obtaining information by unauthorized access to a Web site or database, because sending a text message “is essentially a one-way communication that does not implicate the obtaining of information” from the recipient's device. The court also rejected the plaintiff's claims that the sending of the messages resulted in damage or loss cognizable under the CFAA.

Czech v. Wall Street On Demand, Inc., 2009 U.S. Dist. LEXIS 114125 (D. Minn. Dec. 8, 2009) Download PDF

PRIVACY

Assent to Newspaper’s Online Privacy Policy Did Not Constitute Waiver of Right to Anonymous Speech

An anonymous commenter's assent to a newspaper's online privacy policy did not constitute a waiver of the commenter's right to anonymous speech, a district court ruled. The court found that a contractual waiver of a constitutional right must be clear, but that the language relied upon by the plaintiff seeking the identity of the commenter consisted of only “two sentences in a two-page document in which the overarching theme is that information provided by a user of the site may be used for various commercial purposes.” The court concluded that given the presumption against waiver of a constitutional right, and the “boiler-plate nature” of the language upon which the plaintiff relied, it could not be concluded that the commenter made a knowing waiver of the right to anonymous speech.

Sedersten v. Taylor, 2009 U.S. Dist. LEXIS 114525 (W.D. Mo. Dec. 9, 2009) Download PDF

Editor's Note: The opinion does not identify the specific language upon which the plaintiff relied in arguing that the anonymous poster waived his or her privacy rights, but the plaintiff's brief points to the following provision: "WE ALSO RESERVE THE RIGHT TO USE, AND TO DISCLOSE TO THIRD PARTIES, ALL OF THE INFORMATION COLLECTED FROM AND ABOUT YOU WHILE YOU ARE USING THE SITE IN ANY WAY AND FOR ANY PURPOSE."

Two Circuit Courts Counter the Ninth Circuit on Plain View Exception to Warrant Requirement in Computer Searches

In United States v. Comprehensive Drug Testing, Inc. (9th Cir. Aug. 26, 2009), the U.S. Court of Appeals for the Ninth Circuit, sitting en banc, limited the scope of searches for digital evidence by defining a set of procedures to be followed by law enforcement in requesting and executing such searches. In particular, the Ninth Circuit constrained law enforcement reliance on the plain view exception to the Fourth Amendment warrant requirement in the case of searches for digital evidence. Two U.S. Circuit Courts of Appeal, the Seventh and the Fourth, recently issued rulings diverging from the approach taken by the Ninth Circuit. In United States v. Mann (7th Cir. Jan. 20, 2010), the Seventh Circuit expressly rejected the Ninth Circuit approach, ruling that a police officer did not exceed the scope of a warrant authorizing a search for images taken surreptiously of women in locker rooms when he electronically scanned, indexed and catalogued all files on the computer into viewable format. In United States v. Williams, the Fourth Circuit held that even if a warrant authorizing the seizure of evidence of a harassment crime did not encompass images of child pornography, the seizure of those images fell within the plain view exception to the warrant requirement, because the warrant "impliedly authorized officers to open each file on the computer and view its contents, at least cursorily, to determine whether the file fell within the scope of the warrant's authorization."

United States v. Mann, 592 F.3d 779 (7th Cir. Jan. 20, 2010) Download PDF

United States v. Williams, 592 F.3d 511 (4th Cir. Jan. 21, 2010) Download PDF

Expectation of Privacy in Computer Files Negated by P2P User's Failure To Engage Program Privacy Feature

A federal agent's access to a user's computer via a peer-to-peer file-sharing program did not violate the Fourth Amendment, because the user's expectation of privacy in the contents of his computer was negated by his failure to properly engage the privacy features in the program, the U.S. Court of Appeals for the Ninth Circuit ruled. The court noted that despite the user's efforts to protect his files from access, his files were “entirely exposed to public view” by anyone using the same P2P program. The user's subjective intent not to share his files, the court concluded, did not create an objectively reasonable expectation of privacy. The court also rejected the argument that the agent's use of a specialized forensic software program unavailable to the general public to examine the contents of the files on the user's computer rendered the search unlawful.

United States v. Borowy, 595 F.3d 1045 (9th Cir. Feb. 17, 2010) Download PDF

No Warrant Required for Law Enforcement Access to Cellular Location Data

A criminal defendant's Fourth Amendment rights were not violated when law enforcement agents obtained cellular location data from his cell phone provider without a warrant, the Supreme Court of Georgia ruled. The court noted that at the time the agents asked the provider to “ping” the defendant's cell phone in order to discern his location, he was in a car on a public roadway. The court concluded that the defendant had no reasonable expectation of privacy in his location when he was at a place that was open to visual surveillance.

Devega v. State of Georgia, 689 S.E.2d 293 (Ga. Feb. 1, 2010)

Editor's Note: The subject of warrantless searches of cellular location information is also before the U.S. Court of Appeals for the Third Circuit in In re Application of the United States of America, No. 08-4227 (Third Cir.). The Government is appealing a district court order requiring law enforcement agents to obtain a warrant in order to obtain cell site data from a cellular carrier. The issues are discussed on the Proskauer New Media and Technology law blog.

No Reasonable Expectation of Privacy in Contents of Shared Folder Accessible via Unsecured Wireless Router

A defendant had no reasonable expectation of privacy in the contents of a shared folder that was accessible via an unsecured wireless router to which his computer was connected, a district court ruled. The court found that neither the Fourth Amendment nor the Electronic Communications Privacy Act were violated when a neighbor who inadvertently accessed proscribed images of children via the defendant's wireless network summoned police who viewed them as well. The court found that because the defendant's wireless router was not password-protected, anyone within an approximate 400-foot range around his house could access it. Although the router was by default not password-protected, the court noted that the manual that came with the router contained detailed instructions on how to password-protect it, and emphasized the importance of doing so. The court also noted that forensic examination revealed that the defendant's iTunes application was purposefully set to allow sharing of files contained in the folder in which the subject files were found.

U.S. v. Ahrndt, 2010 U.S. Dist. LEXIS 7821 (D. Ore. Jan. 28, 2010) Download PDF

Under Pennsylvania Law, No Tort Action Lies for Internet Posting of External Photographs of Residence

Taking external photographs of a private residence and making the photographs available on a publicly accessible Web site does not give rise to a tort action under Pennsylvania law, the U.S. Court of Appeals for the Third Circuit ruled. The court concluded that the homeowners' privacy was not invaded because such conduct would not be “highly offensive to a reasonable person” so as to give rise to an intrusion upon seclusion claim. The court similarly concluded that the homeowners had failed to establish a claim for publicity given to private life. The court reversed the lower court dismissal of the homeowners' trespass claim, however, finding that their claim that the vehicle from which the photographs were taken had entered into their private driveway was a trespass claim “pure and simple.”

Boring v. Google, 2010 U.S. App. LEXIS 1891 (3d Cir. Jan. 28, 2010) (unpublished) Download PDF

U.S. Supreme Court Grants Petition for Certiorari in Quon v. Arch Wireless Case Involving Employee Communications Claim under Stored Communications Act

The U.S. Supreme Court granted the petition for certiorari filed by the employer in a case involving the privacy of employee communications under the Stored Communications Act provisions of the Electronic Communications Privacy Act. The Ninth Circuit ruled in Quon v. Arch Wireless Operating Co., Inc. (9th Cir. June 18, 2008), that the contents of an employee's pager text messages archived on the servers of a text messaging provider are protected from disclosure to the employer subscriber of the text messaging service under the SCA. The appeals court held that the pager text messaging provider was an "electronic communication service" within the plain language of the SCA, and therefore that the contents of archived text messages could be disclosed only to "an addressee or intended recipient" of the text messages, i.e. the employee user, not the employer subscriber to the text messaging service. The appeals court also ruled that under the particular facts presented, the subscriber to the text messaging service, a municipal police department, violated the Fourth Amendment rights of the employee user of the text messaging service when the department reviewed the contents of the messages in order to determine whether they were work-related. The court concluded that although the police department had an announced policy disclaiming any employee expectation of privacy in messages using the text messaging service, the "operational reality" was that the department had led employees to believe that such messages would be reviewed only under certain narrow circumstances.

City of Ontario v. Quon, No. 08-1332 (U.S. cert. granted Dec. 14, 2009)

Assistant United States Attorney's Communication with Private Attorney via Employer's E-Mail System Did Not Waive Attorney-Client Privilege

An Assistant United States Attorney who communicated with his private attorney via his government-provided e-mail address did not thereby waive his attorney-client privilege in the contents of the e-mail messages sent to his attorney, a district court ruled. The court concluded that the AUSA "reasonably expected" that his e-mails would remain confidential, because he asserted that he did not realize that his employer would be regularly accessing and saving e-mails sent from his account. The court noted that the Department of Justice had a policy that did not ban personal use of an employee's e-mail account.

Convertino v. United States Department of Justice, 2009 U.S. Dist. LEXIS 115050 (D. D.C. Dec. 10, 2009) Download PDF

ECPA Not Applicable to ISP's Alleged Disclosure of Communications to Foreign Government

The Electronic Communications Privacy Act does not apply to the actions of an ISP that allegedly revealed subscribers' personal information and communications to a foreign government, where the acts of disclosure and interception took place in a foreign country, a district court ruled. The court noted that there is a presumption that U.S. laws apply only within the territorial jurisdiction of the United States, unless a contrary affirmative intention on the part of Congress is clearly expressed. In the case of the ECPA, the court concluded, there is no language in the statute or any indication in the legislative history of the Act that Congress intended the Act to apply extraterritorially, nor is there any basis for extending the Act extraterritorially as a matter of policy. The court also rejected the argument that the Act applied because some of the subscribers' communications may have traveled over the ISPs servers within the United States, because the alleged disclosures and interceptions occurred in the foreign country.

Zheng v. Yahoo! Inc., 2009 U.S. Dist. LEXIS 111886 (N.D. Cal. Dec. 2, 2009) Download PDF

ELECTRONIC MARKETING

Business Owner Held Not Individually Liable for Multimillion Dollar Judgment under Iowa Anti-Spam Statute

A joint owner of a corporate entity was not properly held individually liable for a multimillion dollar judgment under the Iowa anti-spam statute because there was no evidence that she initiated the sending of the spam e-mails in question, the U.S. Court of Appeals for the Eighth Circuit ruled. The court found that the statute imposes liability on a person who “uses an interactive computer service” to “initiate the sending” of spam e-mail, and that the owner's conduct did not fall within the plain meaning of the statutory terms “initiate” and “send.” The court rejected the lower court's theory that the joint owner could be held liable under civil conspiracy or aiding and abetting theories because the statute does not create a civil cause of action for such conduct.

Kramer v. Perez, 2010 U.S. App. LEXIS 3324 (8th Cir. Feb. 19, 2010) Download PDF

Spam Sent via Fake Profiles on Social Networking Site Held Actionable under California Law as Common Law Fraud

A defendant who created numerous fake profiles on a social networking site in order to send unsolicited commercial e-mail messages is liable in an action brought by the operator of the site for common law fraud and deceit under California law, a district court ruled. In granting the operator's motion for entry of a default judgment, the court found that the defendant misrepresented himself to the social networking site as well as to the other users of the site, that other users were tricked into clicking on links to an adult dating site that were contained in the defendant's e-mails, and that he intended the other users to rely on his misrepresentations that he was a legitimate user of the site. The court found that the operator was injured by the defendant's actions in that server response time was decreased, a higher level of bandwidth was used on the site, the operator was forced to hire additional personnel to monitor and stop spamming by the defendant and others, users and potential users were deterred from using the site, and there was attendant damage to the operator's good will and reputation. The court also sustained the operator's claims under the federal CAN-SPAM Act, the California anti-spam act, and the federal Computer Fraud and Abuse Act.

Tagged, Inc. v. Does 1 through 10, 2010 U.S. Dist. LEXIS 5428 (N.D. Cal. Jan. 25, 2010)
Download PDF

TCPA Applies to Text Messages for Which Called Party Is Not Charged

The Telephone Consumer Protection Act, which prohibits the transmission of a “call” using an “automatic telephone dialing system” without the prior consent of the called party, applies to a text message for which the called party is not charged, a district court ruled. The court noted that although the language of the Act was capable of being construed so as to apply only to calls where the calling party was charged, that construction was precluded by a 1992 amendment to the TCPA which gave the Federal Communications Commission the authority to exempt such non-charged calls from the scope of the Act. The court further noted that while the FCC had suggested in a 2003 Report and Order that non-charged calls did not fall within the scope of the Act, that suggestion did not specifically exempt such calls, and the court need not give deference to such a “bare announcement” by a regulatory agency. The court rejected the argument that in enacting and amending the TCPA, Congress was concerned primarily with the cost-shifting to consumers, commenting that “Congress was just as concerned with consumers' privacy rights and the nuisances of telemarketing.”

Abbas v. Selling Source, LLC, 2009 U.S. Dist. LEXIS 116697 (N.D. Ill. Dec. 14, 2009) Download PDF

Editor's Note: In addition to its ruling on the issue of applicability of the TCPA to non-charged calls, the court also explicitly agreed with the reasoning of the Ninth Circuit in Satterfield v. Simon & Schuster (9th Cir. 2009), that text messages are "calls" within the meaning of the TCPA.

California Anti-Spam Statute Not Preempted by Federal CAN-SPAM Act

Claims under California Business & Professions Code Section 17529.5, the California anti-spam statute, are not preempted by the federal CAN-SPAM Act, a district court ruled. Noting the divergent rulings in the Northern District of California on the issue, the court agreed with the opinions that have broadly construed the exception to preemption for state laws that prohibit "falsity or deception in any portion of a commercial electronic message." Consequently, the court concluded, the California statute is not preempted by the CAN-SPAM Act even though plaintiffs are not required to plead and prove the reliance and damages elements of common law fraud.

Asis Internet Services v. Subscriberbase, Inc., 2009 U.S. Dist. Ct. 112852 (N.D. Cal. Dec. 4, 2009) Download PDF

Editor's Note: Asis is a frequent plaintiff in anti-spam cases. In a recent case involving Asis, the Ninth Circuit affirmed a district court ruling that Asis lacked standing under the CAN-SPAM Act because it failed to show harm within the meaning of the Act as a result of the defendant's e-mails. Asis Internet Services v. Azoogle.com, Inc., 2009 U.S. App. LEXIS 26232 (9th Cir. Dec. 2, 2009) (unpublished), citing Gordon v. Virtumundo, Inc., 575 F. 3d 1040, 1049 (9th Cir. 2009). Gordon is another frequent plaintiff in anti-spam cases, and another suit by Gordon was also summarily dismissed pursuant to the Virtumundo opinion. See Gordon v. SubscriberBase Holdings, Inc., 2009 U.S. Dist. LEXIS 115514 (E.D. Wash. Dec. 11 2009).

Massachusetts Law Prohibiting Dissemination of Matter Harmful to Minors Inapplicable to Text and Instant Messages

The Massachusetts statute that criminalizes the dissemination of “any matter harmful to minors” is inapplicable to electronically transmitted text or online instant messaging conversations, the Massachusetts Supreme Judicial Court ruled. The court noted that the statutory definition of “matter” includes “handwritten or printed material” and “visual representations,” but does not include language that would encompass online electronically transmitted conversations. The text and instant messages in question were not “visual representations,” the court found, because that term referred to photographs and other images, not text. Nor did the messages constitute “handwritten or printed material,” as defined by dictionaries or prior judicial opinions construing those terms, the court concluded.

Commonwealth v. Zubiel, 456 Mass. 27, 2010 Mass. LEXIS 24 (Mass. Feb. 5, 2010)
Download PDF

Editor's Note: In a ruling several days after the ruling in Zubiel, a Massachusetts trial court ruled that the creation and transmission of a photograph to a minor via a cellular phone fell within the “harmful to minors” statute, because the statutory definition of “visual material” expressly included computer images. The court also took judicial notice of the fact that “many of the devices we commonly refer to as cellular telephones have the technological capabilities of computers,” and thus fell within the statutory definition of “visual material,” which includes “pictures—moving or still, whether on paper, film or computer.” Commonwealth v. Romero, 26 Mass. L. Rep. 458, 2010 Mass. Super. Lexis 22 (Mass. Super. Ct. Feb. 11, 2010)

ELECTRONIC RECORDS AND SIGNATURES

FACTA Credit Card Truncation Requirements Do Not Apply to E-Mail Order Confirmations

The requirement of the Fair and Accurate Credit Transactions Act that certain credit and debit card information be truncated on printed receipts does not apply to e-mail order confirmations, a district court ruled. The court found that such confirmations are not "electronically printed" within the meaning of FACTA because the plain meaning of the term "printed" (which is not defined in FACTA) encompasses the transfer of information to paper and does not include display of information on a computer screen. The court also found that an e-mail order confirmation is not provided "at the point of sale or transaction" within the meaning of FACTA, relying on prior opinions that concluded that, in context, the term was intended to refer to in-store transactions where the customer is present when the sale is made.

Shlahtichman v. 1-800 Contacts, Inc., 2009 U.S. Dist. LEXIS 112379 (N.D. Ill. Dec. 2, 2009) Download PDF

Editor's Note: This ruling is discussed more fully on the Proskauer Privacy Blog.

Arizona State Bar Ethics Opinion Approves Electronic Client File Storage

Arizona attorneys may provide online storage of client documents provided that they take reasonable precautions to protect the security and confidentiality of those documents and periodically review the reasonableness of those precautions, the State Bar of Arizona stated in a Formal Opinion. The opinion responded favorably to an inquiry from an attorney who wished to provide online access to clients to enable their review of their documents and information. The opinion indicated that the planned system met the requirements of ethical rules and prior opinions on the topic because it utilized Secure Socket Layer encryption, utilized randomly generated alpha-numeric passwords and file folder names, and converted client documents to PDF format that required an additional password to access. The opinion cautioned that it should not be assumed that the system would satisfy security requirements indefinitely and that the attorney should periodically review the security of the system "as technology advances occur."

State Bar of Arizona Ethics Committee Opinion No.09-04 (Dec. 2009)

New York Insurance Department Opinion Controls Validity of Electronic Signature on Clickwrap Insurance Application

The New York State Insurance Department may impose a requirement that an insurance company verify the identity of a person providing an electronic signature on an online application for insurance, notwithstanding the less restrictive definition of an electronic signature in the New York Electronic Signatures and Records Act, a district court ruled. The court noted that while the New York ESRA was amended in 2002 to remove language pertaining to verification of identity from the definition of an electronic signature, the Department could impose such a requirement under its regulatory authority over the business of insurance. The court concluded that there was a disputed issue of fact that precluded the grant of summary judgment on the issue of whether the submission an insurance application via a "standard internet click-through process" satisfied the identity verification requirement, where the process required the applicant to submit personal information including an address and Social Security number.

The Prudential Insurance Company of America v. Dukoff, 2009 U.S. Dist. LEXIS 117843 (E.D. N.Y. Dec. 18, 2009) Download PDF

DOMAIN NAMES AND TRADEMARKS

Domain Names Subject to Judgment Execution Proceedings Where Registry Is Located

A domain name is property of a debtor that is properly subject to judgment execution proceedings in the jurisdiction where the domain name registry is located, the U.S. Court of Appeals for the Ninth Circuit ruled. The court noted that under federal law, judgment execution proceedings are conducted in compliance with the law of the forum state; but California, where the registry for the .com names in question is located, contains no provision concerning execution on domain names. The court concluded that it could properly analogize to the Anticybersquatting Consumer Protection Act, which allows in rem proceedings against infringing domain names and which provides for jurisdiction in the place where the domain name registry is located. The court also opined in dicta that it saw "no reason why" domain names could not also be considered located where the relevant domain name registrar is located.

Office Depot v. Zuccarini, 2010 U.S. App. LEXIS 4052 (9th Cir. Feb. 26, 2010) Download PDF

Domain Name Registrar Not Immune from Trademark Owner's Infringement, ACPA Claims

A domain name registrar that registered numerous infringing domain names, provided private registration services in conjunction with a related entity that concealed the identity of the registrants, and received fees when ads on sites connected to the infringing domain names were clicked, may be liable under the Lanham Act and the Anticybersquatting Consumer Protection Act, a district court ruled. The court found that the trademark owner had sufficiently alleged a "use in commerce" for purpose of a trademark infringement claim by alleging that the registrar and its related entity had cooperated with another defendant and with fictitious entities to profit from the infringing use of the plaintiff's trademarks. The court similarly concluded that the registrar was not automatically entitled to the "safe harbor" for domain name registrars under the ACPA because the trademark owner alleged that the registrar was part of a scheme to profit from the use of the infringing domain names.

Transamerica Corp. v. Moniker Online Services, LLC, 2009 U.S. Dist. LEXIS 114973 (S.D. Fla. Dec. 4, 2009) Download PDF

Computer File Extension Functional, Therefore Not Protectable as Trademark

A computer file extension is inherently functional, therefore a software company that utilizes a particular file extension to designate files that are accessed by its proprietary software may not protect the letters comprising the file extension as a trademark, a district court ruled. The court noted that there are a limited number of letters available to designate file types, and commented: "no one has ownership of file extension designations under the Lanham Act because such designations are inherently functional. Any programmer or computer user anywhere is free to designate file extensions as they see fit, without worrying about trademark violations. File extensions are functional, and functional uses cannot be trademarked."

Autodesk, Inc. v. Dassault Systemes Solidworks Corp., 2009 U.S. Dist. LEXIS 121541 (N.D. Cal. Dec. 31, 2009) Download PDF

Trademark Owner's Reports of Infringing Goods to Online Auction Anti-Infringement Program Protected by "Interested Party" Privilege from Defamation Claim

A trademark owner's reports of infringing goods to an online auction's anti-infringement program were privileged under California law, a district court ruled. The court dismissed the defamation claims of a seller whose auctions were removed from the site and whose account was suspended for a period of time as a result of the trademark owner's reports. The court found that both the online auction site and the trademark owner had an interest in preventing counterfeiting and trademark infringement, and that the reports were made without malice and in furtherance of that interest, therefore they fell within the statutory privilege under Cal. Civ. Code § 47(c). The court similarly dismissed the seller's claims of intentional and negligent interference with prospective advantage, because, among other reasons, with the dismissal of his defamation claims, the seller could not show any wrongful conduct on the part of the trademark owner.

Tommy Bahama Group, Inc. v. Sexton, 2009 U.S. Dist. LEXIS 112452 (N.D. Cal. Dec. 3, 2009) (opinion of magistrate judge) Download PDF

DEVELOPMENTS OF NOTE

Supreme Court Affirms Federal Court Copyright Jurisdiction over Settlement of Claims Involving Unregistered Works

Reed Elsevier Inc. v. Muchnick, No. 08-103 (U.S. Mar. 2, 2010)

UK Courts Have Jurisdiction over Prosecution of Racially Inflammatory Material Created in England, But Published on Web Site Servers Located in the U.S.

Regina v. Sheppard, [2010] EWCA Drim 65 (29 January 2010) (England and Wales Ct. App.)

Rescuecom Abandons Trademark Lawsuit against Google over Adwords Sales

Blog Post

Independent Review Panel Says ICANN Should Reconsider Refusal of Application for .XXX Domain

ICANN Blog Post

Complaint over Allegedly Defamatory “Tweet” Dismissed for Insufficiently Pleading Defamation

Horizon Group Management LLC v. Bonnen, (Ill. Circuit Ct. Illinois Cty Jan. 11, 2010) Blog Post

Second Circuit Rules Antitrust Action against Recording Companies for Internet Music Pricing Stated a Claim under Section 1 of the Sherman Act

Starr v. Sony BMG Music Entertainment et al., No. 08-5637 (2d Cir. Jan. 13, 2010)

National Federation of the Blind Settles Lawsuit against Universities over Planned Use of Electronic Textbooks

Press Release

Illinois Appeals Court Upholds Dismissal of Action Seeking Recovery of Internet Gambling Losses from Credit Card Companies

Reuter v. MasterCard International, Inc., No. 5-07-0372 (Ill. App. Ct. 5th Dist. Jan. 5, 2010)

Federal Acquisition Regulation Amended to Require IT Product Compliance with IPV6 Standard

Federal Register

Florida Ethics Authority Issues Opinion Regulating Social Network Contacts between Judges and Attorneys

Opinion

Related Professionals

- **Jeffrey D. Neuburger**
  Partner
- **Robert E. Freeman**
  Partner
- **Daryn A. Grossman**
  Partner