Proskauer

New Media, Technology and the Law

December 2008

COPYRIGHT

Limiting Online Coupon Downloads via a Software Key May "Effectively Control" Access to and Use of Work under DMCA Anticircumvention Provisions

An online coupon provider's method of limiting the number of downloads of online coupons via a software key may constitute a technological measure that "effectively controls" access to and use of protected works within the meaning of the anticircumvention provisions of the Digital Millennium Copyright Act, a district court held. The defendant was accused of violating the provisions by distributing software that removed the key generated by the plaintiff's software to third parties. The court concluded that the defendant's assertions that the software controlled both the number of copies of coupons that a particular computer could generate, and the overall number of coupons that could be generated "as a whole," sufficiently alleged a cause of action under both DMCA §1201(a) and §1201(b).

Coupons, Inc. v. Stottlemire, 2008 U.S. Dist LEXIS (N.D. Cal. Nov. 6, 2008). Download PDF

Ex Parte Temporary Restraining Order against Sale of Pirated Videogame Prior to Release Justified Where "Marketing Benefit" Would Be Impaired

The issuance of an *ex parte* temporary restraining order against the seller of pirated copies of an unreleased video game is justified where the sale of the pirated game diminishes the videogame developer's "marketing benefits" and undermines the resources for developing games, a district court ruled. The court found that the developer had shown a likelihood of success on its copyright claims and on its claims that the defendant violated the Digital Millennium Copyright Act by advertising the service of modifying game systems to play the pirated copies of the developer's games. The court also ruled that the *ex parte* order was proper because, if the defendant was given notice of the action, there was a risk that he would destroy the offending materials.

Epic Games, Inc. v. Altmeyer, 2008 U.S. Dist. LEXIS 89758 (S.D. Ill. Nov. 5, 2008). Download PDF

First Sale Doctrine Limits Copyright Protection Only for Software Manufactured in the United States

Under §109(a) of the Copyright Act, title to a particular copy of copyrighted software passes after a first sale by the copyright holder only for domestically made copies of U.S.-copyrighted works, a district court held. The court rejected the argument that under §109(a) the defendant, who purchased copies of software made abroad and licensed for sale abroad and sold it within the United States, was entitled to dispose of "lawfully made" copies of copyrighted software in any manner he chose. The court granted summary judgment to the copyright holder, concluding that purchasers of software made outside the U.S. are ineligible to claim the first sale defense to infringement.

Editor's Note: Having ruled that §109(a) was inapplicable, the court concluded that it was unnecessary to reach the plaintiff software distributor's argument that the first sale doctrine was not applicable in any event because the software in question was distributed under a license, not sold, and therefore no "sale" took place.

Microsoft Co. v. Intrax Group Inc. d/b/a Surplus Computers, et al., 2008 U.S. Dist. LEXIS 83756 (N.D. Cal. Oct. 6, 2008). Download PDF See also *Microsoft v. Big Boy*, 2008 U.S. Dist. LEXIS 97965 (S.D. Fla. Dec. 1, 2008) (rejecting first sale defense where software was manufactured and distributed abroad).

TRADEMARKS AND DOMAIN NAMES

Deep Linking May Constitute Trademark Infringement or Dilution, Where Consumer Confusion or False Impression of Affiliation May Result

A real estate company's use of deep links to a trademark owner's Web site to advertise its real estate services may result in trademark infringement and dilution if consumer confusion or a false impression of affiliation results from the linking, a district court ruled. The court refused to dismiss the complaint by a law firm concerning the real estate company's use of its trademark in articles about real estate transactions and accompanying deep links to the biographies of its attorneys who participated in the transactions. The court concluded that the deep links to the law firm's Web site could create the false impression that the law firm endorsed or is affiliated with the real estate firm, or could create consumer confusion. The court also concluded that the real estate company's assertion of the nominative fair use defense and the statutory exclusion for news reporting and news commentary required the resolution of legal and factual issues that could not be adjudicated on a motion to dismiss.

Jones Day v. Blockshopper LLC d/b/a Blockshopper.com, et al., 2008 U.S. Dist. LEXIS 94442 (N.D. Ill. Nov. 13, 2008). Download PDF

Mention of a Competitor's Trademark in a Web Site Disclaimer May Generate "Initial Interest Confusion"

A product manufacturer's use of a competitor's trademark in a Web site disclaimer gave rise to initial interest confusion because Internet search engines would return the manufacturer's Web site in the results of searches including the competitor's trademark, a district court ruled. The dispute arose when the manufacturer, which formerly distributed the competitor's products, continued to use domain names incorporating the competitor's trademarks in order to "maintain a presence for customers with warranty claims" with respect to previously sold goods. The court granted summary judgment on the competitor's trademark infringement claims with respect to the warranty language based on consumer confusion, but declined to grant summary judgment with respect to the competitor's cyberpiracy claims. The court concluded that the issue of whether the manufacturer's continued use of the domain names was in "bad faith" within the meaning of the Anticybersquatting Consumer Protection Act was a fact issue for the jury, commenting that the use of the competitor's trademark in the disclaimer was subject to "competing inferences" with respect to the issue of bad faith.

Suarez Corp. Industries & MHE Corp. v. Earthwise Technologies, Inc., 2008 U.S. Dist. LEXIS 92931 (W.D. Wash. Nov. 14, 2008). Download PDF

In Domain Name Dispute, Trademark Owner's Failure to Plead a Claim under the ACPA Precludes an Award of Damages under the ACPA

A trademark owner's failure to plead violations of the Anticybersquatting Consumer Protection Act (ACPA) in its complaint precludes the grant of statutory damages under the ACPA, despite the fact that the trademark owner properly pleaded and proved trademark infringement, a district court ruled. The court found that the owner had properly pleaded and proved trademark infringement and unfair competition by the domain name registrant, and that entry of a default judgment on those claims was proper. The court also found, however, that the trademark owner had not included allegations of cyberpiracy in its complaint, either by specific reference to the ACPA or by general reference to cyperpiracy, nor did the trademark owner's complaint allege the elements necessary to establish an ACPA claim. The court ruled that the trademark owner would be permitted to submit evidence establishing its actual damages or the domain owner's profits pursuant to its trademark infringement claim.

Kwik-Sew Pattern Co. v. Derek Gendron, et al., 2008 U.S. Dist. LEXIS 94125 (W.D. Mich. Nov. 19, 2008). Download PDF

No Bad Faith as a Matter of Law Where Authorized User of Trademark in Vanity Phone Number Used Number as Domain Name

A car recycler that was granted permission to use a 1-800 phone number containing a car manufacturer's trademark in a prior settlement agreement did not act in bad faith as a matter of law when it used the vanity phone number as a domain name, a district court ruled. The court denied both parties' motions for summary judgment on the car manufacturer's cyberpiracy claims with respect to the registration of the www.800allaudi.com domain name. The court reasoned that in light of its previous finding that the terms of a settlement agreement unambiguously granted the car recycler permission to use the vanity telephone number 1-800-All-AUDI, it could not find as a matter of law that the registration of a domain name with the contents of that vanity telephone number, which the defendant had a legal right to use, constituted bad faith within the meaning of the Anticybersquatting Consumer Protection Act. The court commented that subjective issues such as good faith are "singularly inappropriate for determination on summary judgment."

Audi AG v. Shokan Coachworks, Inc., 2008 U.S. Dist. LEXIS 92021 (N.D.N.Y. Oct 12, 2008). Download PDF

Kentucky Court Rules It Has Subject Matter and *In Rem* Jurisdiction in Civil Forfeiture Proceeding Seeking Seizure of Illegal Gaming Domain Names

Kentucky courts of general jurisdiction have subject matter and *in rem* jurisdiction over civil forfeiture proceedings seeking seizure of the domain names through which illegal gambling was conducted in that state, a Kentucky trial court ruled. The court upheld its prior *ex parte* order in which the Commonwealth of Kentucky sought seizure of 141 domain names alleged to connect users to illicit gambling Web sites. The court reasoned that domain names are property which is present in Kentucky, and as such, can be the subject of an *in rem* proceeding there. The court further held that its *ex parte* seizure order did not offend due process because shutting down illicit gaming is an important government interest, and the domain names could be removed from the reach of the government if advance notice were given. The court did rule that gaming Web site owners could avoid forfeiture, however, by installing geographic blocks preventing Kentucky residents from accessing their Web sites. With respect to the argument that a forfeiture of domain names would create havoc on the Internet, the court commented:

"This doomsday argument does not ruffle the court. The Internet, will all its benefits and advantages to modern day commerce and life, is still not above the law, whether on an international or municipal level. The challenge here is to reign in illegal activity and abuse of the Internet within the framework of our nation's and Commonwealth's existing common law norms and principles, until expressed guidelines from state and federal legislative bodies say otherwise."

Commonwealth v. 141 Internet Domain Names, Case No. 08-CI-1409 (Ky Cir. Ct., Oct. 16, 2008). Download PDF

Editor's Note: On November 14, a Kentucky appeals court granted a stay of the scheduled forfeiture hearing in order to permit an immediate appeal of the issue of the trial court's jurisdiction over the proceeding. Oral argument on the appeal was held on December 12.

Cybersquatting Claim against Domain Name Registered Prior to Plaintiff's Use of Trademarks Not Supported by ACPA

A plaintiff that did not acquire rights in its “cosmopolitan” trademarks until a year after the registration of the “cosmopolitanresort.com” domain name may not sustain an action against the domain name registrant under the Anticybersquatting Consumer Protection Act, a district court ruled. The court concluded that to prevail on a cybersquatting claim, the ACPA requires the plaintiff’s trademark to be “distinctive” or “famous” at the time of registration of the domain name. The court ruled that the developer’s marks were not distinctive or famous because they did not exist at the relevant time, nor is the term “cosmopolitan,” standing alone. distinctive or famous in real estate services. The court dismissed the plaintiff’s ACPA claim but declined to dismiss trademark infringement claims, finding that there were genuine issues of material fact with respect to the timing of the use of the trademark, whether the defendant’s use of the Web site hosted at “cosmopolitanresort.com” was “in commerce,” and whether the real estate developer can prove that the marks had secondary meaning prior to the date the defendant began using the disputed domain name.

3700 Associates, LLC v. Griffin et al., 2008 U.S. Dist. LEXIS 79721 (S.D. Fla. Oct. 6, 2008).

ONLINE CONTENT

Identities of Anonymous Posters Who Made Allegedly Defamatory Statements Concerning a Public Official Not Protected by the First Amendment

A government official who was accused of sexual misconduct by anonymous posters on an Internet forum had the right to compel the disclosure of their identities because their comments exceeded the protection afforded by the First Amendment to criticism of public officials, a Pennsylvania court ruled. Citing the ruling in the same court in *Polito v. AOL Time Warner*, the court determined that the official could obtain the identities of the posters if she (1) stated a cognizable claim under Pennsylvania law, (2) demonstrated that the identifying information is directly related to the claim and fundamentally necessary to secure relief, (3) sought the information in good faith, and (4) was unable to determine their identities in another way. The court found that six of the posts could satisfy the elements for a prima facie case for defamation per se under Pennsylvania law because they alleged serious sexual misconduct.

Pilchesky v. Gatelli, No. 07-CV-1838 (Pa. Ct. Common Pleas Lackawanna Cty Oct. 1 2008).
Download PDF

Pages Printed from State's Official Web Site Are Self-Authenticating under Federal Rules of Evidence

Electronically stored information printed from a state public authority's Web site is self-authenticating and admissible under the Federal Rules of Evidence, a district court ruled. The court held that information printed from the Maryland Judiciary Case Search Web site that contained a caption identifying the source of the information was self-authenticating under Fed. R. Evid. 902(5) as a publication purporting to be issued by a public authority. The court also concluded that information printed from a password-protected Web site hosted by a subdivision of a state agency and obtained through a state freedom of information act request is similarly self-authenticating, even though the information was not subject to unrestricted publication to the general public.

Williams v. Long, 2008 U.S. Dist. LEXIS 91110 (D. Md. Nov. 7, 2008).

Wikipedia Encyclopedia Not a "Reliable Website" of Which Judicial Notice May Be Taken

The Wikipedia encyclopedia is not a "reliable website" for purposes of taking judicial notice, a Texas appeals court ruled. The appellant, who was appealing his conviction for possession with the intent to deliver cocaine, requested that the appeals court take judicial notice of a Wikipedia entry concerning the "John Reid" technique that allegedly results in false confessions to support his claims that his confession was involuntary and coerced. The court commented that the Wikipedia encyclopedia is not reliable because anyone, even an anonymous party, may edit a Wikipedia entry.

Flores v. State, 2008 WL 4683960 (Texas Ct. App. Oct. 23, 2008) (unpublished). Link

In Web Site Defamation Case, Florida Supreme Court Rejects False Light Tort as Potentially Chilling to First Amendment Speech

In a case involving an alleged defamatory statement published in a newsletter posted on an Internet Web site, the Florida Supreme Court ruled that the tort of false light invasion of privacy is not a recognized cause of action in Florida because it is duplicative of existing torts. The court also concluded that that recognizing a separate false light tort could chill free speech under the First Amendment because the "highly offensive to a reasonable person" standard under the false light tort is not entirely clear, and because the tort is not limited by the same safeguards and protections that have been established in defamation cases. The court also ruled, however, that the appropriate standard in assessing whether a defamatory statement tends to injure the plaintiff's reputation is whether the statement prejudices the plaintiff in the eyes of a "substantial and respectable" minority of the community.

Jews For Jesus, Inc. v. Rapp, 2008 Fla. LEXIS 2010 (Fla. October 23, 2008). Download PDF

PATENTS

Application for Patent on Business Method Properly Rejected, Where "Machine or Transformation" Test Not Satisfied

An application for a patent on a method of hedging risk in the field of commodities trading was properly rejected where the process claimed in the application failed to meet the "machine or transformation" test, the Court of Appeals for the Federal Circuit ruled. The court upheld the rejection of the application by the patent examiner and the Board of Patent Appeals and Interferences, on the ground that a process claim constitutes eligible subject matter only if it is tied to a particular machine or transforms a particular article into a different state or thing. The court rejected several other tests for determining the patentability of a claimed process, including the "useful, concrete and tangible result" test articulated in the court's prior ruling in *State Street Bank & Trust Co. v. Signature National Bank*.

In re Bilski, 2008 U.S. App. LEXIS 22479 (Fed. Cir. Oct. 30, 2008)

Editor's Note: The *Bilski* ruling is discussed more fully in the Proskauer Client Alert, "In re Bilski: Federal Circuit Affirms Patent Office in Narrowing Scope of Patentable Subject Matter."

CFAA

Employee's Unauthorized Access to a Company Computer to Delete Personal E-mails Lacked Intent to Defraud Necessary for a Violation of the Computer Fraud and Abuse Act

The founder of a company who allegedly remotely accessed his work computer after he left the company in order to delete e-mails stored in his Outlook folder did not demonstrate the necessary intent to defraud to sustain an action by the company under the Computer Fraud and Abuse Act, a district court held. The court dismissed the company's claims based on the CFAA, noting that although the plaintiff's access to the computer after he left the company was clearly unauthorized, he did not access sensitive material with an intent to defraud. The court further found that his behavior did not amount to trespass to chattels because the company did not allege that the deleted files were significant to the business of the company and instead his behavior was nothing "other than harmless intermeddling with the computer system."

Hecht v. Components International, Inc., 2008 NY Slip. Op. 28439 (N.Y. Supreme Court Nov. 6, 2008).

Computer Used to Conduct E-mail Correspondence and Fund Remittance in Interstate Commerce Qualifies as a Protected Computer under the CFAA

An employer's complaint alleging that the employer's laptop used to conduct e-mail correspondence and fund remittances in interstate commerce was accessed by an employee in order to delete and shred substantial files pertaining to the employer's financial status sufficiently alleged a cause of action under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (a)(2)(C), a district court held. The court found that the laptop qualified as a protected computer because the defendant was authorized to use it in interstate commerce to communicate with the employer's customers and to transfer funds in interstate commerce. The court also found that the employee's conduct also involved interstate commerce, because the defendant unlawfully accessed the employer's online bank account, obtained financial information, and transferred funds to herself and her creditors. Finally the court found that the employer successfully pleaded damages in excess of the statutory $5,000 in the form of the funds the employer had to expend to recover the deleted records.

Patrick Patterson Custom Homes, Inc. v. Bach, 2008 U.S. Dist. LEXIS 92761 (N.D. Ill. Nov. 14, 2008). Download PDF

CFAA Claim Need Not Be Pleaded with Particularity

A claim under the federal Computer Fraud and Abuse Act is not a "fraud" claim that must be pleaded with particularity under Fed. R. Civ. P. 9(b), a district court ruled. The court noted that only one of the CFAA subsections cited in the complaint mentions fraudulent conduct, and that section references an intent to defraud, which the court concluded may be pleaded generally. The court found that allegations that the defendants, without authorization or in excess of their authorization, accessed the plaintiff's online bank account, changed the user name and password, and falsely manipulated financial information to divert assets; accessed the plaintiff's computer with the intent to defraud in order to obtain confidential business and financial information and install malicious software programs that enabled remote access; and caused damage in excess of $5,000 in one year as a result, made out a plausible claim to relief against the defendants.

Zero Down Supply Chain Solutions, Inc. v. Global Transportation Solutions Inc., 2008 U.S. Dist. LEXIS 84722 (D. Utah Oct. 17, 2008). Download PDF

Insurance Company Not Required To Defend Claims against Internet Advertiser under Computer Fraud and Abuse Act for Alleged Installation of Spyware

An insurance company is not obligated to defend an Internet advertiser against a lawsuit seeking damages under the Computer Fraud and Abuse Act for installation of spyware on the plaintiff's computer that allegedly caused it to freeze and process so slowly as to become essentially inoperable, a district court held. The court noted that the advertiser's general liability policy expressly excluded claims for losses to software, and that the complaint alleged that the spyware affected only the software on the plaintiff's computer, not the hardware. The court also concluded that while the errors and omissions policy did not exclude damage to software, the complaint did not allege any "error, unintentional omission or negligent act" within the meaning of the policy because the plaintiff claimed that the advertiser intentionally placed the spyware on the plaintiff's computer.

Eyeblaster, Inc. v. Federal Insurance Co., 2008 U.S. Dist. LEXIS 81912 (D. Minn. Oct. 7, 2008). Download PDF

PRIVACY

Individualized Nature of ECPA Claims against SEC-Regulated Broker-Dealer and Investment Adviser for E-Mail Interception Precludes Class Certification

Claims under the Electronic Communications Privacy Act (ECPA) against an SEC-regulated broker-dealer/investment adviser alleging unlawful interception of e-mails without consent are highly individual and fact-specific, and therefore they do not meet any of the Fed. R. Civ. P. 23(a) prerequisites for class certification, a district court held. The action was brought by representatives of the entity who claimed that e-mail interception and forwarding conducted by the entity for purposes of compliance with SEC regulations was unlawful and sought to join not only other representatives and employees of the entity, but also all parties who sent or received e-mail from such persons. The court concluded that among the individualized issues was whether those potential plaintiffs, such as the plaintiffs who were contractually obligated to provide the entity with copies of their e-mails, had a reasonable expectation of privacy in the contents of the e-mails.

Murray v. Financial Visions, Inc., 2008 U.S. Dist. LEXIS 93419 (D. Az. Nov. 6, 2008) (unpublished). Download PDF

Editor's Note: The broker-dealer/investment adviser defendant also argued that the plaintiffs' ECPA claims should be dismissed because the subject e-mails were in electronic storage and therefore could not have been "intercepted" within the meaning of the Wiretap Act provisions cited by the plaintiffs. In the absence of evidence describing the process of transmission and interception of the subject e-mails, the court declined to dismiss the plaintiffs' claims, but commented that in light of the Ninth Circuit's interpretation of the Wiretap Act in *Konop v. Hawaiian Airlines*, it was "skeptical" of the validity of the plaintiffs' Wiretap Act claims.

Access to Former Employer's E-Mail System via Another's Credentials Violates Stored Communications Act, not Wiretap Act

A former employee who used another employee's username and password to access the former employer's e-mail system after he left the company violated the Stored Communications Act because his continued access was unauthorized within the meaning of the Act, a district court ruled. The court found that the former employee's unauthorized access was knowing and intentional, commenting that not only was it "common sense" that the access was wrongful, but the e-mail login page displayed a banner stating that access was for the company's employees only. The court dismissed the SCA claims against a competitor of the employer to whom the former employee gave certain of the e-mails, finding that the SCA punishes only "access," not disclosure and use of the information accessed. The court also dismissed claims under the Wiretap Act, finding that neither the employee nor the competitor "intercepted" any messages in transmission. The court declined to dismiss claims under the Tennessee Personal and Commercial Computer Act because, the court found, the language of that statute presented "various potential avenues" by which the employer could convince a jury, based upon the facts presented, that the Act had been violated by one or more of the defendants.

Cardinal Health 414, Inc. v. Adams, 2008 U.S. Dist. LEXIS 84713(M.D. Tenn. Oct. 10, 2008). Download PDF

Search Warrant Not Required for Seizure of a Cell Phone's Contents Made Pursuant to Valid Traffic Stop

Under the Fourth Amendment, a search warrant is not required for the seizure of information from a cell phone pursuant to a valid traffic stop, so long as probable cause exists under the Fourth Amendment's automobile exception, a district court ruled. The court held that if a law enforcement officer has the requisite probable cause to believe that evidence of a crime would be found, then the automobile exception allows for the search and downloading of information from a suspect's cell phone. Here, the court upheld the recovery of a cell phone's contact list, dialed numbers, and recent calls. The court also summarily rejected the argument that the seizure of a cell phone's contents violated the Electronic Communication Privacy Act, finding that law enforcement officials did not "intercept" electronic communications within the meaning of the Act.

United States v. Rocha, 2008 U.S. Dist. LEXIS 77973 (D. Kan. Oct. 2, 2008). Download PDF

SPAM

ISP Must Allege “Specific Harms” for Standing under CAN-SPAM Act

An Internet Service Provider’s complaint under the federal CAN-SPAM Act does not establish the ISP’s standing where it fails to allege “specific harms” that show that the ISP has been “adversely affected” within the meaning of the Act, a district court ruled. The court dismissed the ISP’s complaint with leave to amend, finding that the ISP’s allegations of harm under the Washington Commercial Electronic Marketing Act and the Washington Consumer Protection Act were similarly deficient. Noting a prior similar ruling involving the same ISP, the court directed that the ISP’s amended complaint satisfy the requirements of that ruling, i.e., that the complaint specify the specific time frame in which the e-mails alleged to violate the statutes were sent, the addresses and domain names that received the e-mails, and a brief summary of the factual basis upon which the ISP claimed the defendant sent the e-mails.

Gordon v. SubscriberBASE Holdings, Inc., 2008 U.S. Dist. LEXIS 88214 (E.D. Wash. Oct. 31, 2008).

Editor’s Note: The plaintiff James Gordon has brought numerous CAN-SPAM actions with varying degrees of success on the question of standing. Compare *Gordon v. Virtumundo*, 2007 U.S. Dist. LEXIS 35544 (W.D. Wash. May 15, 2007) (finding no standing) with *Gordon v. Ascentive*, 2007 U.S. Dist. LEXIS 44207 (E.D. Wash. June 19, 2007) (finding standing). Oral argument on his appeal in *Gordon v. Virtumundo* was held in the Ninth Circuit on December 9.

“Internet Access Service” Entitled to Standing under CAN-SPAM Act Not Limited to Internet Access Provider

An “Internet access service” entitled to bring suit under the federal CAN-SPAM Act includes a proxy service that enables end users to access blocked Internet content, a district court ruled. The court noted that Congress could have limited standing under the Act to an “Internet Service Provider,” the narrower and better known term, but the use of the broader term “Internet access service” suggested an intent to more broadly define the entities entitled to standing. The court found that even though subscribers to the proxy service had to use another service to get access to the Internet, the service provided by the proxy Web site fell within the broader statutory term.

Haselton v. Quicken Loans, Inc., 2008 U.S. Dist. LEXIS 81126 (W.D. Wa. Oct. 14, 2008). Download PDF

Editor's Note: This case is discussed more fully on the Proskauer Privacy Law blog.

State Law Action for Alleged Deception in Web Site Membership Solicitation E-Mails Preempted by Federal CAN-SPAM Act

An action brought under California anti-spam act alleging that membership solicitation e-mails sent by a Web site were false, deceptive and misleading is preempted by the federal CAN-SPAM Act, a district court ruled. The court noted that the complaint alleged that the defendant membership Web site, pursuant to its Terms of Service, scraped its members' address books and then sent membership solicitations to those addresses, making it appear that the solicitation was from the member. The court found that while the messages were alleged to be misleading, the plaintiffs did not make any claims that satisfied the elements of common law fraud or deceit. Because the federal CAN-SPAM Act preempts state statutes that regulate commercial e-mails except where those statutes prohibit fraud or deceit, the court concluded that the state law claims were preempted.

Hoang v. Reunion.com, 2008 U.S. Dist. LEXIS 85187 (N.D. Cal. Oct. 3, 2008) Download PDF

SOFTWARE LICENSING

Under Indiana Law, Fraud Not Established by Failure to Honor Software Contract "90-Day Satisfaction Guarantee"

A software distributor's alleged failure to honor a "90-day satisfaction guarantee" with respect to its software does not constitute fraud but is "nothing more than a broken promise," a district court ruled. In dismissing the software buyer's fraud counterclaim, the court found that under Indiana law, a finding of actual fraud may not be based upon "representations of future conduct, on broken promises, or on representations of existing intent that are not executed." The court declined to dismiss the buyer's breach of contract counterclaims, however, finding that the distributor had failed to show that the parties intended a complete integration pursuant to which the 90-day guarantee was excluded from the parties' subsequent written agreement.

Digitech Computer, Inc. v. Trans-Care Inc., 2008 U.S. Dist. LEXIS 88214 (S.D. Ind. Oct. 14, 2008). Download PDF

ELECTRONIC RECORDS AND ELECTRONIC DISCOVERY

Federal Court Plaintiff May Rely on Digital Audio Record in Trial in Lieu of Submission of Printed Transcript

A plaintiff in a post-trial motion in a federal court may rely on the audio record of a jury trial which resulted in a verdict, a district court held. The court concluded that reliance on the digital audio record was proper due to permission granted by the Judicial Conference of the United States to federal district courts to rely on digital audio recording as a substitute for court reporters. The court noted that the trial was short and the plaintiff's motion focused on a discrete portion of the trial record and the audio record was readily available to the court and its personnel for reference. However, the court emphasized that its ruling concerned only post-trial motions at its level, and not appeals.

K.R. v. School District of Philadelphia, 2008 U.S. Dist. LEXIS 91423 (E.D. Pa. Nov. 5, 2008). Download PDF

No Waiver of Privilege in Electronic Documents Where Interests of Justice Outweigh Deficiencies in Party's "Reasonable Steps" to Prevent Inadvertent Disclosure

Deficiencies in a party's undertaking of "reasonable steps" to prevent inadvertent disclosure of privileged electronic documents should not result in a waiver of privilege where the interest of justice weighs heavily against waiver, a district court ruled. In applying a five-factor test to determine reasonableness, the court extensively analyzed the conduct of electronic discovery and found that the steps taken by the party to prevent disclosure were, to some extent, not reasonable. However, the court held that the fifth factor, the interest of justice, strongly favored the inadvertently disclosing party. The court commented that "loss of attorney-client privilege in a high-stakes, hard-fought litigation could lead to severe prejudice," and that denial of the inadvertently disclosed documents was not prejudicial to the adverse party, as it had neither a right nor an expectation to them.

Rhoads Industries, Inc. v. Building Materials Corp. of America, et al., 2008 U.S. Dist. LEXIS 93333 (E.D. Pa. Nov. 14, 2008). Download PDF

ONLINE COMMERCE

Economic Presence Alone Is Sufficient to Establish a Substantial Nexus with a State, Allowing It to Impose Tax Obligations Pursuant to the Commerce Clause

Economic presence alone is sufficient to establish the substantial nexus requirement for a state to impose tax obligations on an out-of-state financial institution pursuant to the Commerce Clause, the Indiana Tax Court held, siding with a recent holding in West Virginia. MBNA Bank issued credit cards to Indiana residents, and in doing so regularly solicited business from customers in the state, exceeded a *de minimis* number of clients and regularly received interest and fees from them. The court held that these ties, while not physical, constituted a substantial nexus with Indiana, permitting the state to impose excise tax on the bank.

MBNA America Bank, N.A. & Affiliates v. Indiana Department of State Revenue, 2008 Ind. Tax LEXIS 27 (Ind. Tax Ct. Oct. 20, 2008). Link

Limiting Consumers' Alternatives in Voice and Data Services and Cell Phone Application Aftermarkets Are Grounds for Antitrust Suit

A cell phone manufacturer and telecommunications provider exercised market power in the aftermarkets for voice and data services and phone applications by limiting consumer alternatives, thus giving consumers sufficient grounds to state a claim for violation of Section 2 of the Sherman Act, the district court held. The court concluded that upon signing up for a two-year voice and data plan with ATTM (AT&T Mobility) which, unbeknownst to consumers, had a five-year iPhone distribution exclusivity provision in its agreement with Apple, purchasers of the SIM-locked device were deprived of freedom in the aftermarket. Further, the court concluded that through contracting, technological controls and software updates, Apple limited consumers' choice of iPhone applications to those in which it maintained a financial interest. In both aftermarkets, the court held, Apple and ATTM had exercised enough market power to give consumers sufficient grounds for a Sherman Act claim.

In re Apple & AT&TM Antitrust Litigation, 2008 U.S. Dist. LEXIS 88923 (N.D. Ca. Oct. 1, 2008) Download PDF

Editor's Note: The court also denied the defendants' motion to compel arbitration, finding that the arbitration agreement included in the voice and data plan terms of service was unconscionable under California, New York and Washington law, and that the unconscionability laws of those states were not preempted by the Federal Arbitration Act.

Joint Venture of Digital Media Companies Charging Supracompetitive Prices for Internet Music Is Not in Violation of Sherman Act

Digital music companies that charged, through a joint venture, supracompetitive prices for Internet music were found not to have violated Section 1 of the Sherman Act, as the circumstances were insufficient to allow inference of an agreement, a district court held. The court concluded that under the U.S. Supreme Court ruling in *Bell Atlantic v. Twombly*, a Section 1 Sherman Act claim must allege "some form of concerted action between at least two legally distinct economic entities," and if tacit collusion or conscious parallelism in their actions is alleged, there must be "more than a bare showing of parallel conduct." The court held that maintaining supracompetitive prices, which may be against the companies' self-interest, by parallel conduct in a highly concentrated market with high barriers to entry was not sufficient to establish a preceding agreement without further context.

In re Digital Music Antitrust Litigation, 2008 U.S. Dist. LEXIS 79764 (S.D.N.Y. Oct. 9, 2008) Download PDF

JURISDICTION

Court Has Subject-Matter Jurisdiction in Trademark Infringement Action against Pollster's Pakistan-Located Web Site Using Protected "Gallup" Mark

A polling company located in Pakistan that used the protected “Gallup” trademarks on its Web site committed sufficient infringing acts within the United States to establish subject-matter jurisdiction over the Gallup Company’s trademark infringement and unfair competition claims, a district court ruled. The court found that it was not necessary to consider the Paskistani polling company’s argument that there was no basis for the court to exercise extraterritorial jurisdiction under the Lanham Act. The court noted that the appropriate jurisdictional test is whether defendants’ alleged trademark infringement occurred “in commerce.” The defendants’ prominent display of the “Gallup” mark on their Web site, gallup.com.pk, adversely affected commerce in the United States, the court concluded, providing subject-matter jurisdiction over Gallup’s claims that that the defendants’ Web site infringed on their trademark.

Gallup, Inc. v. Business Research Bureau (PVT.) Ltd. et al, 2008 U.S. Dist. Lexis 93462 (N.D. Cal. Nov. 10, 2008). Download PDF

Jurisdiction Not Established under Ohio Long-Arm Statute by Alleged Online Defamation, Where Web Site Operator Did Not Offer Goods or Services

An Ohio resident claiming that she was defamed by content posted on an out-of-state Web site failed to establish jurisdiction under the Ohio long-arm statute, where the defendant Web site operator offered only content and did not offer any goods or services for sale or lease, a district court ruled. The court also found that the long-arm statute was not satisfied because the operator's out-of-state conduct was not “inherently associated” with the forum state. In addition, the court stated that, even if personal jurisdiction could have been established under the long-arm statute, the requirements of due process were not met because, although the alleged defamatory content concerned an Ohio resident, the content did not concern the resident’s Ohio activities, the Web site was not specifically directed at Ohio, and the operator’s conduct took place outside of Ohio.

Wargo v. Lavandeira, 2008 U.S. Dist. LEXIS 80592 (N.D. Ohio Oct. 3, 2008).

Blogger Not Subject to Specific Jurisdiction in California, Absent Showing That Alleged Defamation Was Purposefully Directed at Forum State

Specific jurisdiction was not established where the plaintiff in a defamation suit failed to provide evidence that the defendant non-resident blogger had expressly aimed his conduct at California when he published defamatory statements about the plaintiff, a district court ruled. The plaintiff alleged that the blogger had published numerous defamatory statements on his blog, which he then promoted by a technique known as “google bombing,” i.e., linking the statements to other Web sites and search engines in order to assure that statements would be returned in searches of the plaintiff’s name. While the court found that the plaintiff had proved intentional conduct on the part of the defendant and thus the first prong of the three-part “Calder effects test” had been satisfied, the lack of evidence supporting a finding that the defendant intentionally targeted the plaintiff, knowing that she was a resident of the forum state, was fatal to a finding of jurisdiction.

Fahmy v. Hogge, 2008 U.S. Dist. LEXIS 87103 (C.D. Cal. October 14, 2008).

Editor’s Note: See also *Williams v. Advertising Sex LLC*, 2008 U.S. Dist. LEXIS 77719 (N.D. W. Va. October 3, 2008) (finding that specific jurisdiction was not properly exercised over a Web site operator who sold downloads of a fake sex tape that purportedly depicted the plaintiff and mentioned the name of the forum state, where the overall content of the Web site did not have a strongly local character and was not intentionally targeted at or focused on the forum state).

Specific Jurisdiction in Online Trademark Infringement Case Satisfied Due Process Where Web Site Is Accessible in the Forum State

The due process clause is not offended by the exercise of specific jurisdiction over an out-of-state defendant who is alleged to have infringed the plaintiff’s trademarks on his Web site that was accessible in the forum state, the Court of Appeals for the Eleventh Circuit ruled. The court noted that the plaintiff alleged that the defendant, a manager of musicians, posted an endorsement by a former client using that client's trademarks without that client's permission. The court ruled that under the “Calder effects test” adopted by the Ninth Circuit, the plaintiff’s allegations constituted “express aiming,” in that the defendant individually targeted the plaintiff in order to misappropriate his name and reputation for commercial gain, and that this conduct was calculated to cause injury to the plaintiff in the forum state.

Related Professionals

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