Proskauer

New Media, Technology and the Law

August 2008

Merely "CC-ing" In-House Attorney on E-Mail Does Not Establish Attorney-Client Privilege in a Communication

The attorney-client privilege is not applicable to e-mail correspondence requested from an insurance provider in the course of litigation involving an insurance coverage dispute governed by New Jersey law, merely because the insurer's in-house attorney was copied on the e-mails, a district court ruled. In assessing the applicability of the privilege to e-mails reviewed in camera, the court reasoned that the privilege should not apply unless the e-mail in question was either directed to or sent by the attorney. The court also concluded that even if an e-mail is deemed privileged, documents attached to the e-mail must be evaluated separately to determine if the privilege is independently applicable to the document.

Editor's Note: This is an important ruling that both attorneys and clients should keep in mind. It is often assumed that when an attorney is copied on an e-mail, the e-mail becomes subject to the attorney-client privilege. This assumption is particularly questionable in the case of in-house counsel who have business management or related functions. The general assumption has been soundly discredited in this opinion, which also rejects the related misconception that if an e-mail is subject to the attorney-client privilege, any attachment is privileged as well. As a matter of good practice, if an e-mail is intended to be subject to the attorney-client privilege, at a minimum it should be sent from or to an attorney.

Spiniello Companies v. The Hartford Fire Insurance Co., 2008 U.S. Dist. LEXIS 53509 (D.N.J. July 14, 2008) (unpublished)

Federal Circuit Rules Open Source License Terms are Enforceable Under Copyright Law

The terms of the open source Artistic License, which limit the right to modify and distribute licensed software code, are conditions that limit the scope of the license grant and therefore can be enforced under copyright law, the Court of Appeals for the Federal Circuit held. The court concluded that Artistic License, which permits the modification and distribution of the code but requires that distributors include certain information with any distribution, "on its face ... creates conditions." The court also referenced the use of the term "conditions" in the license language, as well as other language consistent with the creation of a license condition under California law. The court broadly endorsed the use of open source licenses for the distribution of copyrighted works, commenting that authors "who engage in open source licensing have the right to control the modification and distribution of copyrighted material."

Editor's Note: This is an extremely important ruling, one of a very few involving open source licenses, and the first by a U.S. court to squarely rule that open source licenses are enforceable under copyright law. See further discussion on the New Media and Technology Law blog.

Jacobsen v. Katzer, 2008 U.S. App. LEXIS 17161 (Aug. 13, 2008)

Second Circuit Rules Cable Company's Remote Storage Digital Video Recorder System Does Not Directly Infringe Copyright

The remote storage digital video recorder (RS-DVR) system proposed to be provided by a cable company to its subscribers to permit the remote networked storage of television programs for playback does not directly infringe the copyright of program providers, the Second Circuit ruled. The appeals court reversed the ruling of the district court, which granted summary judgment in favor of the program providers and an injunction on the grounds that the system created unauthorized, infringing copies and violated the program providers' right of public performance when the copies were played back by cable company subscribers. Among other things, the appeals court concluded that the RS-DVR system's copying of 1.2 seconds at a time of program content into system RAM, for a period of 0.1 seconds, did not meet the definition of a "copy" in the Copyright Act, because the copies were not embodied "for a period of more than transitory duration."

Editor's Note: Of particular interest in this ruling is the appeals court's limitation of the Ninth Circuit opinion in *MAI Systems Corp. v. Peak Computer* (9th Cir. 1993), and its conclusion that the Ninth Circuit failed to address the duration requirement for determining whether a copy is sufficiently fixed. The Second Circuit concluded that while computer RAM copying may result in the creation of a "copy" within the meaning of the Copyright Act, it does not do so as a matter of law.

The Cartoon Network LP, LLP v. CSC Holdings, Inc., 2008 U.S. App. LEXIS 16458 (2d Cir. Aug. 4, 2008)

Circuit Court Approves Lenient Sentence for DMCA Criminal Charges

A district court did not abuse its discretion in sentencing a defendant convicted of violating the anticircumvention provisions of the Digital Millennium Copyright Act (DMCA) to non-custodial community service, restitution and supervised release, the Ninth Circuit ruled. The defendant had been convicted of selling over $1 million worth of counterfeit "access cards" that allowed purchasers to circumvent the access protection on the DirecTV digital satellite feed. The appeals court noted that the district court had concluded, among other things, that the violations of which the defendant was convicted did not "pose the same danger to the community as many other crimes." Judge Bybee dissented, noting that the defendant had bragged that he had made over $400,000 from the sale of the cards.

U.S. v. Whitehead, 2008 U.S. App. LEXIS 14889 (9th Cir. July 14, 2008)

No Waiver of U.S. Sovereign Immunity for Claims Under DMCA

The U.S. Government has not waived its sovereign immunity with respect to claims under the Digital Millennium Copyright Act, the Federal Circuit ruled. The court concluded that the Court of Federal Claims properly dismissed claims brought by the assignee of a software program alleging that the U.S. Air Force had appropriated the program source code and modified it to defeat an expiration date feature. The court concluded that the assignee's copyright infringement claims were properly dismissed because they did not fall within the express waiver contained in 28 U.S.C. § 1498(b) for certain copyright claims. The court also pointed out that unlike 28 U.S.C. § 1498(b), the DMCA does not contain any express waiver of sovereign immunity. Further, the court noted that the DMCA prohibits certain actions by individual persons, not the Government, and it provides for actions to be brought in a district court, not in the Court of Claims. The court also concluded that the assignee's DMCA claims were not encompassed in the 28 U.S.C. § 1498(b) express waiver for copyright claims, because the DMCA created new claims for liability that are separate and distinct from claims for copyright infringement.

Blueport Co. v. U.S., 2008 U.S. App. LEXIS 15787 (Fed. Cir. July 25, 2008)

Availability of Work on Web Site Does Not Give Rise to Implied License, Entry Into Public Domain

The fact that a copyrighted work was available on the author's publicly accessible Web site does not give rise to an implied license to reproduce the work, a district court ruled. The court rejected the argument proffered by the defendant in a copyright infringement action that the author granted an implied license by allowing "unfettered downloads" of the work. The court noted that an implied license arises only in "narrow circumstances" involving the creation of a work at the request of another party, and that the defendant had made no showing that such circumstances were present with respect to the work in question. The court also rejected the argument that the posting of the work on the plaintiff's Web site resulted in the work entering the public domain, noting that the term is one of art under the Copyright Act that references the expiration of an author's exclusive rights, a circumstance not involved in the present case.

Thornton v. J. Jargon Co., 2008 U.S. Dist. LEXIS 52396 (M.D. Fla. July 8, 2008)

Web Site Posting of Audio Excerpt of Radio Program Protected by Fair Use Defense

The posting of a four-minute audio clip taken from a two-hour radio program in order to explain objections to the remarks of the radio commentator is protected by the fair use defense, a district court ruled. The court concluded that the radio commentator had failed to show that the defendants posted the audio clip for any reason other than criticism of or comment on the commentator's views, thus the purpose and character of the use weighed heavily in favor of the defendants. The court also concluded that the amount of the work copied in relation to the whole was small, rejecting the radio commentator's argument that each copied portion of the entire program should be viewed as a separate and distinct work that was copied in its entirety. The court found that the posting of the clip had no actual or potential market impact on the original work because its usage was limited to public criticism. With respect to the posting of the actual audio excerpts, the court commented that their use was not "unreasonable ... since they reaffirmed the authenticity of the criticized statements and provided the audience with the tone and manner in which the plaintiff made the statements."

Savage v. Council on American-Islamic Relations, Inc., No. C 07-6076 (N.D. Cal. July 25, 2008)

Government Employee Had No Reasonable Expectation of Privacy Where Explicit Warning Was Displayed on Computer Login

A government employee had no reasonable expectation of privacy in his work computer, where the system displayed a warning banner every time the employee logged on to the computer, a district court ruled. The court noted that the warning banner displayed text, to which the user had to assent before proceeding, stating that the computer was for official use only, that unauthorized access or use was subject to prosecution, that information could be monitored, intercepted or disclosed, including for purposes of criminal prosecution, and expressly stating that a user had "no expectation of privacy under this system."

United States v. Mosby, No. 3:08-CR-127 (E.D. Va. July 25, 2008)

Anonymous Blog Posters Entitled to Notice of Discovery Efforts Aimed at Identification

A magistrate judge's order directing a deponent to answer questions that could lead to the identification of parties who posted anonymous blog comments should be vacated in order to allow notice to be given to the anonymous posters so that they may file objections to the requested discovery, a district court ruled. The court noted that there were questions as to whether the deponent, who refused to answer deposition questions on First Amendment grounds related to the right to comment anonymously, had standing to assert the rights of the anonymous posters. Nevertheless, the court concluded that it had the authority to adopt a procedure to protect against potential violations of third-party rights, and that there was "at least good reason to believe" that the anonymous posters would object to their identities being revealed. The court also concluded that in assessing the discoverability of the identities of the anonymous posters, the magistrate judge to whom the matter was assigned should follow the standard set out by the Delaware Supreme Court in *Doe v. Cahill*, requiring the plaintiff to submit evidence sufficient to overcome a limited motion for summary judgment with respect to its underlying claims.

Editor's Note: The opinion contains a helpful analysis of the various standards adopted by courts in assessing the discoverability of the identity of anonymous posters.

Quixtar v. Signature Management Team, 2008 WL 2721265 (D. Nev. July 7, 2008)

Civil Subpoena to ISP for Discovery of Party's E-Mail Messages Barred by Federal SCA

A subpoena issued pursuant to Fed. R. Civ. P. 45 to an Internet Service Provider by the plaintiff in a civil action, seeking discovery of the defendant's e-mail messages, is precluded by the Stored Communications Act (SCA), a district court ruled. The court agreed with the defendant that subpoena should be quashed because the SCA precludes the ISP from disclosing the stored contents of her e-mail, regardless of any claimed relevance to the plaintiff's action. The court noted that the civil subpoena did not fall into any of the limited exceptions to the general prohibition in the SCA. The court also ruled that the subpoena should be quashed on the alternate ground that it subjected the defendant to an undue burden, because the request encompassed any e-mails over a six-year period and constituted "the all too familiar fishing expedition which this court does not countenance."

Editor's Note: The question of whether the SCA precludes the use of a Fed. R. Civ. P. 45 civil discovery subpoena to an ISP has arisen in prior cases. See Neuburger & Garde, "Court Refuses to Enforce Discovery Subpoena Against E-Mail Service Provider," (Washington Legal Foundation Legal Backgrounder Sept. 1, 2006).

Hone v. Presidente U.S.A., Inc., 2008 U.S. Dist. LEXIS 55722 (N.D. Cal. July 21, 2008)

Attorney May Be Liable for Disclosing Protected Health Information Obtained in Discovery to Prosecutor

An attorney who disclosed a patient's protected health information obtained in the course of a divorce and custody proceeding to the prosecutor in a criminal case against the patient may be liable for the unauthorized disclosure, the Supreme Court of Ohio ruled. The court reasoned that the disclosure of the records in the divorce and custody proceeding was proper because the patient had placed his health status into issue in that proceeding and thereby waived his right to confidentiality. However, the court concluded that the patient's waiver was limited to that proceeding. Accordingly, the court concluded that an attorney who disseminates medical information obtained through discovery may be liable for an independent tort for further disclosure of the information.

Editor's Note: In determining that there is a public policy in favor of maintaining the confidentiality of medical information, the court referenced Ohio state laws concerning confidentiality of medical records in various settings, as well as the confidentiality obligations of health care providers under the federal Health Information Portability and Accountability Act of 1996 (HIPAA).

Hageman v. SouthwestGeneralHealthCenter, 2008 Ohio 3343 (Ohio July 9, 2008)

Despite Possibly Unauthorized Gag Order, Administrative Subpoena to ISP for Subscriber Information Was Proper

The inclusion of a non-disclosure directive on an administrative subpoena to an Internet Service Provider seeking subscriber information did not render the subpoena improper, a Hawaii appeals court ruled. The court agreed with the defendant that there was no authority for the inclusion of a directive prohibiting the release of information concerning the subpoena without a court order, but concluded that the inclusion of the non-disclosure directive on the subpoena did not warrant the suppression of the information provided pursuant to the subpoena. The court noted that the disclosure of subscriber information pursuant to an administrative subpoena is authorized under both the federal Electronic Communications Privacy Act and the Hawaii state law equivalent statute, and the subscriber had been informed in the subscriber agreement that information would be supplied pursuant to such a subpoena without notice to the subscriber.

Editor's Note: The viability of "gag orders" accompanying law enforcement subpoenas is a subject of controversy. In May 2008, the Internet Archive partially succeeded in a challenge to a federal gag order issued by the FBI in connection with the service of a National Security Letter on the Archive; the dispute ended in a settlement. In July, a state prosecutor withdrew a demand that bloggers served with a subpoena seeking information on other, anonymous bloggers remain silent about the service of the subpoena.

State of Hawaii v. Offerman, 2008 Haw. App. LEXIS 390 (Haw. Intermediate Ct App. July 17, 2008)

Warrantless Search of Laptop at Border Does Not Violate Fourth Amendment

A search of a defendant's laptop, conducted at an airport by customs officials without probable cause or reasonable suspicion, does not violate the Fourth Amendment, a California appeals court ruled. The court noted the U.S. Supreme Court ruling in *U.S. v. Flores-Montano* authorizing warrantless border searches as an exercise of sovereign authority. The court rejected the argument that a computer is entitled to greater protection because it contains expressive materials, finding that a computer is "the same as any other container for the purposes of search and seizure law." The court also rejected the defendant's analogy to body searches, commenting:

"Indeed, the human race has not yet, at least, become so robotic that opening a computer is similar to a strip search or body cavity search. Of course viewing confidential computer files implicates dignity and privacy interests. But no more so than opening a locked briefcase, which may contain writings describing the owner's intimate thoughts or photographs depicting child pornography."

People v. Endacott, 2008 Cal. App. LEXIS 1068 (Cal. Ct. App. 2d Dist. July 16, 2008)

Online Print-On-Demand Company Not Liable as Publisher

An online print-on-demand company is not liable as a publisher in an action for defamation and other torts brought by the subject of a book printed by the company, a district court ruled. The court concluded that the even if the print-on-demand company is considered a "publisher" of the book in the legal sense, that determination does not itself establish liability for defamation, because under Maine law, there is no liability for defamation without fault. The court noted that the on-demand company's role differed substantially from that of a traditional publishing company in several respects: the on-demand company was paid by authors rather than paying them; the on-demand company published any manuscript submitted to it for publication, without editing, fact-checking or reviewing the manuscript in any way; and the on-demand company did not engage in any marketing efforts on behalf of authors. Thus, the court concluded, the on-demand company did not know or have reason to know of the alleged defamatory statements contained in the book.

Editor's Note: This case is also notable for its ruling that publication of personal information on a MySpace page negates a later claim for the torts of false light invasion of privacy or public disclosure of private facts. See discussion on the New Media and Technology Law blog.

Note also that no claim of immunity under Section 230 of the Communications Decency Act seems to have been raised in this case, an issue upon which Prof. Eric Goldman comments in his blog posts on this case.

Sandler v. Calcagani, 2008 U.S. Dist. LEXIS 54374 (D. Me. July 16, 2008)

New York Enacts Statute Regulating Violent Content on Videogame Consoles

The New York Governor signed into law legislation that establishes an advisory council to conduct a study on the connection between interactive media and real-life violence in minors exposed to such media. The legislation also requires by 2010 that new videogame consoles sold at retail in New York State to incorporate technology that allows the owner to limit access to videogames on the basis of their content, and mandates that games sold at retail in New York State disclose the ratings obtained from the gaming industry's voluntary rating system.

Editor's Note: At least one news report stated that civil rights groups are planning a challenge to the new law.

Chapter 299, Laws of 2008

Claim for Cancellation of Trademark Not Properly Pleaded in Domain Name Dispute

A domain name registrant who was ordered to turn over a domain name in a proceeding under the Uniform Domain Name Dispute Resolution Policy does not have standing to seek a cancellation of the prevailing party's registered trademark in a subsequent federal court proceeding, a district court ruled. The court noted that the basis for the registrant's claim for cancellation was an alleged false statement concerning the trademark owner's status as a successor in interest to the original entity that had rights in the mark. The court ruled that the domain name registrant lacked standing to seek a cancellation of the mark, because he failed to show that he had a "real commercial interest" in the trademark (as opposed to the disputed domain name) that would be damaged in the absence of cancellation.

Future Media Architects, Inc. v. Deutsche Luftansa AG, 2008 U.S. Dist. LEXIS 51741 (S.D.N.Y. July 8, 2008)

SEC Guidance on Company Web Sites Addresses Blogs, Shareholder Forums

The Securities and Exchange Commission voted on July 30 to issue an interpretive release to provide guidance to companies seeking to use their Web sites to provide information to investors. The release addresses such issues as when information posted on a company Web site is considered "public" under Regulation FD; company liability for information on Web sites, including hyperlinks to third-party information, summary information, and the content of interactive Web sites; the types of controls and procedures that are advisable with respect to company information in that context; and the format of such information. In particular, the release reminds companies that federal securities antifraud provisions apply to blogs and shareholder forums, and states that certain disclaimers of liability for blog or forum content "violates the anti-waiver provisions of the federal securities laws."

Commission Guidance on the Use of Company Web Sites, Release No. IC-28351

Allegation that Employee Copied Employer Data to Less Secure Server Makes Out CFAA Claim

A departing employee who allegedly copied confidential and proprietary employer information for the benefit of a new employer is not liable under the Computer Fraud and Abuse Act (CFAA) provision prohibiting unauthorized access or exceeding authorized access to a computer, a district court ruled. In so ruling the court referenced the ongoing disagreement among federal courts over whether the authority of an employee to access a computer is effectively withdrawn by virtue of acts of disloyalty to the employer. The court refused to dismiss a CFAA claim alleging damage to the employer's computer by virtue of the employee's transfer of confidential documents from a secure server to a less secure server in the course of making external copies of the documents that he removed from the employer's premises. The court concluded that such conduct fit the statutory definition of "damage" as "impairment to the integrity or availability of data, a program, a system, or information," and that the legislative history of the CFAA "supports the conclusion that intentionally rendering a computer system less secure" constitutes damage. The court also concluded that the employer had made out a claim under the Tennessee Personal and Commercial Computer Act of 2003.

Editor's Note: Compare the recent ruling in *Mintel International Group, Ltd v. Meesham Neergheen*, 2008 U.S. Dist. LEXIS 54119 (N.D. Ill. July 16, 2008), in which the district court on similar facts involving employee copying of confidential data summarily concluded that the employer had made out a claim that the employee's copying "exceeded authorized access" within the meaning of the CFAA.

Black & Decker (US), Inc. v. Smith, 2008 U.S. Dist. LEXIS 53031 (W.D. Tenn. July 11, 2008)

CFAA Action in Federal Court Not Precluded by Parallel State Action on Similar Claims

A company that instituted an action in state court against former employees alleged to have deleted information from company computers before leaving to form a competing company is not precluded from maintaining a simultaneous federal court action under the Computer Fraud and Abuse Act (CFAA) seeking relief for the same conduct, a district court ruled. The court considered the factors under which federal courts evaluate claims of abstention where a similar or related state action has been filed, and concluded that while the parties were sufficiently identical and the plaintiff sought substantially the same damages in the two actions, the legal claims were not parallel. The court noted that the issue to be litigated in the federal action was the extent of the defendants' authority to delete information from the plaintiff's computers, while the state court action involved a wider scope of claims involving contract law and trade secrets, the existence of a fiduciary relationship between the parties, and the claimed loss of business opportunities. The court also denied the defendants' motion to dismiss the CFAA claims, ruling that the allegations that the defendants deleted data from the employers' computer using a file erasure program and intentionally caused damage without authorization sufficiently alleged a CFAA claim.

Editor's Note: It appears that the plaintiff filed the later, federal action when a preliminary injunction obtained in the earlier-filed state action was stayed on appeal.

Alliance International, Inc. v. Todd, 2008 U.S. Dist. LEXIS 56077 (E.D.N.C. July 22, 2008)

Under New York Law, Limited Time for Exercise of Option for Software Source Code License is Enforceable, Despite "Disproportionate Forfeiture" Claim

Under New York law, a strict time limit on a licensee's exercise of an option to purchase a perpetual license to use a vendor's proprietary security source code is enforceable according to its terms, a district court ruled. The court noted that agreement of the parties was "written in plain English and could not be clearer," and that "New York takes an exceedingly hard line on time-limited options," on the theory that the option holder "has absolute control" over the exercise of the option to the detriment of the giver of the option. The court rejected several equitable arguments raised by the licensee, including the argument that the late exercise of the option should be excused in order to avoid a "disproportionate forfeiture" in the form of the great expense required for the licensee to obtain a substitute product and incorporate it into its own proprietary instant messaging software. The court concluded that the expense of reworking the software would not work a forfeiture because the licensee was free to obtain a substitute product from a different vendor, and because the licensee retained ownership of its own proprietary source code.

Facetime Communications, Inc. v. Reuters Limited, 2008 WL 2853389 (S.D.N.Y. July 22, 2008)

Third Circuit Affirms Permanent Injunction Against COPA Prohibition of Online Content That is "Harmful to Minors"

The Child Online Protection Act (COPA), which imposes civil and criminal penalties on the online posting of information for commercial purposes that is "harmful to minors" is constitutionally infirm because it is not narrowly tailored to serve the government's compelling interest in preventing minors from being exposed to harmful material on the Web, it is not the least restrictive means available to effect that interest, and it is substantially overbroad, the Third Circuit ruled. Reiterating its prior rulings on the statute, the court concluded that the district court was correct in entering a permanent injunction against the enforcement of the statute.

Editor's Note: COPA was enacted in 1998 and was immediately challenged on constitutional grounds. The statute has been the subject of two rulings by the U.S. Supreme Court, *Ashcroft v. American Civil Liberties Union*, 535 U.S. 564 (2002) (remanding for reconsideration of standard under which lower court evaluated constitutionality) and *Ashcroft v. American Civil Liberties Union*, 542 U.S. 656 (2004) (remanding to allow trial on efficacy of blocking and filtering technology). On the second remand, Government efforts to obtain discovery from search engine companies to show the prevalence of objectionable material online yielded the opinion in *Gonzales v. Google, Inc.*, 234 F.R.D. 674 (N.D. Cal. 2006) (restricting Government discovery of search engine user requests and search results).

ACLU v. Mukasey, 2008 U.S. App. LEXIS 15423 (3d Cir. July 22, 2008)

E-Mail Service of Process Sufficient in In Rem Domain Name Action

In an *in rem action* under the federal Anticybersquatting Consumer Protection Act (ACPA), service of process on the domain name registrant is sufficient where the record shows that the plaintiff had e-mail correspondence with the registrant, the registrant agreed to service of process by e-mail when he registered the domain name, and the plaintiff also attempted to serve the registrant at the postal address provided at the time of registration, a district court ruled. The court concluded that the plaintiff had received notice of the pending lawsuit and had been given an opportunity to respond, satisfying the due diligence requirement of the ACPA and the requirements of due process. The court further concluded that under the circumstances, the plaintiff need not publish notice of the pending lawsuit.

Editor's Note: Regarding the issue of publication, the district court noted the reference in the ACPA to publication of notice "as the court may direct," and the conflict in rulings regarding whether such publication is mandatory. Compare *Yahoo!, Inc. v. Yahooahtos.com*, 2006 WL 2303166 (E.D. Va. 2006) (discretionary) with *Shri Ram Chandra Mission v. Shajmarg.org*, 139 F.Supp.3d 721 (E.D. Va. 2001 (mandatory).

Biomedical Technology Solutions, Inc. v. www.demolizer.com, No. 07-cv-02664 (D. Colo. July 18, 2008)

Washington Public Records Act Extends to E-Mail Metadata

An e-mail composed by a private citizen regarding a public controversy, which was sent to the private e-mail address of a deputy mayor and which was discussed by the deputy mayor at a public meeting, falls within the scope of the Washington Public Records Act, as does the metadata associated with the e-mail message, a Washington state appeals court ruled. The metadata at issue included the "To" and "From" information from the original sender, as well as forwarding information. The court concluded that the e-mail constituted a public record because, even though it was created and transmitted by a private citizen, it was "used" by the deputy mayor during a public meeting. The court also concluded that the metadata fell within the scope of the Act because the deputy mayor acted as an agent of the City in using her personal e-mail account for the City's business, and thus the City "owned" the metadata in question.

O'Neill v. City of Shoreline, 2008 Wash. App. LEXIS 1740 (Wash. Ct. App. Div. 1 July 21, 2008)

In Tort Action, Hotel's Use of Hotel Company's E-Mail Domain in Marketing Materials a Factor in Finding Agency Relationship

A hotel's use of an e-mail address containing a hotel company's e-mail domain, and the inclusion of that e-mail address in marketing materials that referred to the hotel as a member of the hotel company's "Luxury Collection," is a factor that, along with other evidence, could support a jury finding of an agency relationship between the hotel and the hotel company, a district court held. The court refused to grant summary judgment dismissing the tort plaintiff's claims against the hotel company predicated on the theory of apparent authority. The court concluded that the use of the domain name coupled with the other evidence suggesting an agency relationship created an issue of fact as to whether the hotel company knew of and acquiesced in the hotel's apparent authority.

Santora v. Starwood Hotels and Resorts Worldwide, Inc., 2008 U.S. Dist. LEXIS 54865 (N.D. Ill. July 16, 2008)

In CAN-SPAM Suit, Over 100 E-Mails Knowingly Sent to Forum State Satisfies "Calder" Jurisdiction Test

Allegations that a sender transmitted over 100 e-mails to a company's employees in violation of the federal CAN-SPAM Act, and that the sender knew the employees were located in the forum state, sufficiently established the "purposeful availment" requirement for the exercise of personal jurisdiction over the sender, a district court ruled. The court concluded that the plaintiff company's allegations satisfied the three-part test established by the U.S. Supreme Court in *Calder v. Jones*, i.e., that the defendant have committed an intentional act, expressly directed at the forum state, causing harm that the defendant knew was likely to be suffered in the forum state.

Melaleuca, Inc. v. Hansen, 2008 U.S. Dist. LEXIS 55951 (D. Idaho July 18, 2008)

Developments of Note

U.S. Patent Office Warns Patent Practitioners on Technology Export Limitations on Outsourcing Searches and Applications Notice

U.S. Commerce Dept Offers Certification Mark for EU Data Protection Safe Harbor Program Participants Announcement

FTC Releases Study on Integrated Advertising of Food Products to Children Report

Copyright Office Says Satellite TV Statutory Licenses Should Be Eliminated Report

New U.S. Law Requires VoIP Providers to Offer 911 Access H.R. 3403 Bill Summary & Status File

Congress Holds Hearings on ISP "Deep Packet Inspection" Hearing Information

U.S. Department of Health & Human Services Settles First HIPAA Privacy Enforcement Action Press Release

U.S. and EU Agree on Principles for Sharing Personal Data for Law Enforcement Purposes Draft Final Report

New York Extends Criminal Impersonation Law to Internet, Electronic Activity Chapter 304 of Laws 2008

Delaware Enacts Law Regulating Internet Pharmacy Sales to Residents Laws 2008 Chapter 410

New York Attorney General Makes Agreements With ISPs on Blocking Child Pornography Press Release

New Mexico Supreme Court Voids Dell Computer Class Action Ban Fisher v. Dell Computer Corp.

Broadcasters Sue RedLasso Video Upload Site Over Web Clips News Coverage

Rosetta Stone Files Keyword Advertising Suit Against Competitor and Affiliate Marketers Complaint

District Court Shuts Down GMAT Exam Test Question Web Site Press Release

Teenager Charged With Felony For eBay Listing of Presidential Vote Gets Community Service News Coverage:

Motion Picture Companies File Copyright Action Against Web Sites Hosting Hyperlinks to Pirated Movies Complaint, Disney Enterprises, Inc. v. FOMDB.com (C.D. Cal. July 29, 2008)

Apple Computer Sues Pystar Over Sales of Mac Clones Complaint

UK Privacy Authority Approves Google Street View Mapping Press Release

UK House of Lords Rejects "Pentagon Hacker" Appeal of Extradition Order Judgment

Italian Prosecutor Charges Google Executives Under Criminal Defamation and Privacy Laws For Taunting Video News Coverage

Subject of Fake Facebook Profile Gets £ 22,000 in UK Lawsuit News Coverage

Related Professionals

Jeffrey D. Neuburger
Partner