Proskauer

New Media, Technology and the Law

July 2010

Edited by **Jeffrey D. Neuburger**

COPYRIGHT

No First Amendment Violation in Statute Restoring Copyright Rights of Foreign Authors

An amendment to the Copyright Act that grants copyright protection to various foreign works that were previously in the public domain in the United States is not violative of the First Amendment, the U.S. Court of Appeals for the Tenth Circuit ruled. The amendment restores copyright rights in foreign works that were formerly in the public domain in the United States for failure to comply with formalities, lack of subject matter protection, or lack of national eligibility. The court concluded that the amendment is a content-neutral regulation of speech, entitled to intermediate scrutiny under the First Amendment, and sustainable if it "advances important governmental interests unrelated to the suppression of free speech and does not burden substantially more speech than necessary to further those interests." The court held that the government had demonstrated a substantial interest in the protection of American copyright holders' interests abroad, and that the amendment was narrowly tailored to protect that interest.

Golan v. Holder, 2010 U.S. App. LEXIS 12641 (10th Cir. June 21, 2010).

Editor's Note: The amendment is Section 514 of the Uruguay Round Agreements Act ("URAA"), Pub. L. No. 103-465, § 514, 108 Stat. 4809, 4976–81 (1994) (codified as amended at 17 U.S.C. §§ 104A, 109). Section 514 was enacted to implement Article 18 of the Berne Convention for the Protection of Literary and Artistic Works, which requires signatories to provide the same copyright protections to authors in member countries that it provides to its own authors.

Web Site Operator's Knowledge of "Generalized Practice" of Copyright Infringement Insufficient to Negate DMCA Safe Harbor

A Web site operator's knowledge of a "generalized practice" of copyright infringement by users of its service is insufficient to deprive it of the protection of the "safe harbor" provided by Section 512(c) of the Digital Millennium Copyright Act, a district court ruled. The court concluded that the references in the statute to "actual knowledge that the material or an activity is infringing" and "facts or circumstances from which infringing activity is apparent," means that the operator must have "actual or constructive knowledge of specific and identifiable infringements of individual items."

Viacom International Inc. v. YouTube Inc., 2010 U.S. Dist. LEXIS 62829 (S.D.N.Y. June 23, 2010).

No DMCA or Trademark Liability for Provider of Online Printing Services for Removal of Material Deemed Infringing

An online printing services provider is not liable for removal of user content that it deems infringing or otherwise objectionable, a district court ruled. Upon notification of a claim from the owner of a registered mark that a design uploaded to the site by a user was infringing, the provider removed the design. The court rejected the *pro se* plaintiff's claim that the removal of the design violated the provider's obligations under the takedown provisions of the Digital Millennium Copyright Act, on the ground that the mark owner asserted only a trademark claim. The court noted that the provider's terms of service and user agreement reserved to it the right to remove content it considered infringing or otherwise objectionable in its "sole and absolute discretion." The court also rejected the user's Lanham Act claim on the ground that he did not have standing under the Lanham Act, and that, in any event, the Lanham Act does not include "put back" provisions such as those contained in the DMCA.

Williams v. Life's Rad, 2010 U.S. Dist. LEXIS 46763 (N.D. Cal. May 11, 2010).

Company That Distributed P2P Software Secondarily Liable for Massive Infringement by Users

A company that created and distributed a peer-to-peer file-sharing program that was used to distribute unauthorized copies of copyrighted music files on a "massive scale" is secondarily liable for acts of direct infringement on the part of the users of the program, a district court ruled. The court found that inducement of infringement was established by evidence that the company knew of the users' infringement, purposefully marketed the software to infringers, profited by selling advertising space on its system and by selling an upgraded version of its program, and failed to implement technologies and measures aimed at mitigating infringement. The court found that foregoing evidence also established that the company had the right and ability to limit the use of its program for infringement and had failed to do so, and thus the company also was vicariously liable for the users' infringement. The court also ruled that the chief executive officer of the company was personally liable for infringement by the company because he directed and benefitted from the company's infringing activities, and had personal knowledge of the infringement. The court declined to grant summary judgment on the issue of contributory infringement, however, due to a lack of evidence on the issue of substantial non-infringing uses for the program.

Arista Records LLC v. Lime Group LLC, 2010 U.S. Dist. LEXIS 46638 (S.D.N.Y. May 11, 2010).

CONTRACTS

Arbitration Clause Referenced in Contract with ISP Binding on Subscriber

An arbitration clause referenced in a business services agreement signed by an Internet services subscriber is enforceable under the Federal Arbitration Act, a district court ruled. The court rejected the argument that the clause was not binding because the subscriber was not given a physical copy of the document in which it was contained, noting that the document containing the clause and the location of the document on the Internet service provider's Web site were expressly referenced in the business services agreement. The court also rejected the argument that the FAA was inapplicable because the agreement did not involve an interstate commerce, finding that an agreement for the provision of telecommunications services, including telephone and Internet service, involves interstate commerce.

Manard v. Knology Inc., 2010 U.S. Dist. LEXIS 60629 (M.D. Ga., June 18, 2010).

Under New York Law, Vendor’s Specific Representations of Software Functionality Support Claim for Fraudulent Inducement

Specific representations made by a salesman concerning the functionality of a software system which the purchaser alleges was inadequate for its purposes support the purchaser's claim for fraudulent inducement, a district court ruled. The court noted that under applicable New York law, a claim of fraudulent inducement requires “an assertion of (1) the misrepresentation of a material fact, (2) known by the defendant to be false and intended to be relied upon when made and (3) justifiable reliance and resulting injury.” The court found that while some of the statements made by the salesman were non-actionable "puffing," the purchaser's complaint detailed specific representations concerning the software functionality that went beyond mere puffing and could be considered statements of fact concerning the capabilities of the software.

Shema Kolainu-Hear Our Voices v. Providersoft, 2010 U.S. Dist. LEXIS 50447 (E.D.N.Y. May 21, 2010).

CONSUMER PROTECTION

Web Site That Created and Delivered Unverified Checks at Direction of Users Violated FTC Act

A company that operated a Web site that created and delivered unverified checks at the direction of users violated the unfair practices provisions of the Federal Trade Commission Act, the U.S. Court of Appeals for the Ninth Circuit ruled. The appeals court noted that evidence showed that the service was extensively used by "unscrupulous opportunists" to create and send fraudulent checks drawn on the bank accounts of numerous victims. The court rejected the company's argument that it had not "caused" injury to consumers within the meaning of the Act because it did not "obtain, input or direct" the delivery of the consumer information used to effectuate the creation of the fraudulent checks. The court found that the company "created and controlled a system that facilitated fraud and that the company was on notice as to the high fraud rate" and continued to create and deliver checks without proper verification.

Federal Trade Commission v. Neovi, Inc., 2010 U.S. App. LEXIS 9888 (9th Cir. May 14, 2010).

COMPUTER FRAUD AND ABUSE ACT

Employee Who Breached Confidentiality Agreement for Benefit of Competitor Exceeded Authorized Access under CFAA

An employer's complaint under the Computer Fraud and Abuse Act that an an employee copied employer trade secrets for the benefit of the employer's competitor, in violation of a broad confidentiality agreement, properly stated a claim that the employee exceeded his authorized access to the employer's computer system, a district court ruled. The court found, however, that the CFAA claim was otherwise defective for failure to properly plead the particular provisions of the Act alleged to have been violated, the specific statutory factors involved and the particular damage suffered, and granted leave to amend.

Marketing Technology Solutions v. Medizine LLC, 2010 U.S. Dist. LEXIS 50027 (S.D.N.Y., unsealed and filed May 18, 2010).

Editor's Note: The court cited the First Circuit ruling in EF Cultural Travel BV v. Explorica, Inc. (1st Cir. 2001) in finding that a violation of a confidentiality agreement renders an employee's access unauthorized under the CFAA. Compare the Ninth Circuit ruling in LVRC Holdings, LLC v. Brekka (9th Cir. 2009), in which the Ninth Circuit ruled that an employee's act of disloyalty to the employer does not render the employee's access to the employer's computer unauthorized within the meaning of the CFAA.

Labor Union E-Mail Campaign Did Not Violate CFAA

A labor union that posted a pre-addressed form e-mail on its Web site, enabling union supporters to e-mail an employer with a pro-union message with "the click of a few buttons," and that allegedly encouraged supporters to inundate the employer's e-mail system with messages, did not violate the federal Computer Fraud and Abuse Act, a district court ruled. The court found that the employer's complaint did not plausibly allege that the union was responsible for knowingly causing a transmission that intentionally damaged the employer's computer in violation of 18 U.S.C. § 1030(a)(5)(A), because the employer's letter demanding that the e-mails stop did not inform the union that the e-mails were damaging to its computer system. The court also dismissed the employer's claim under 18 U.S.C. §§ 1030(a)(5)(B) and (C) for unauthorized access causing damage, because the sending of the e-mails did not constitute "access" to the employer's computers.

Pulte Homes v. Laborers' International Union of North America, 2010 U.S. Dist. LEXIS 46416 (E.D. Mich. May 12, 2010).

Damage, Impairment or Interruption of Service Required to Show Compensable Loss under CFAA

A compensable "loss" under the Computer Fraud and Abuse Act is not established by an allegation that a company spent in excess of $5,000 to investigate unauthorized access to its computerized data, where the company failed to show any underlying damage, impairment or interruption of service to a computer or a computer system, a district court held. The plaintiff company alleged that its former employee accessed its computer assigned design (CAD) system without authorization in order to copy certain CAD data files to use them for the benefit of a competitor. The court noted, however, that the company conceded that its claim of a $5,000 loss was not based upon lost revenue, and was based only on a damage assessment that it claimed was conducted in order to determine the scope of the alleged unauthorized intrusion and whether it resulted in any harm to its files or data. The company did not allege that it had any problems accessing or using its CAD system, the court noted, thus the claimed loss was not compensable under the CFAA.

von Holdt v. A-1 Tool Corp., 2010 U.S. Dist. LEXIS 49071 (N.D. Ill. May 17, 2010).

Cost of Examining Third-Party Computers to Locate and Delete Misappropriated Files Not Compensable under CFAA

A plaintiff who claimed that his files were copied without authorization from a purloined "thumb drive" and onto various third-party computers failed to show a compensable loss under the Computer Fraud and Abuse Act because he failed to show that the thumb drive was somehow damaged or impaired by the defendant's act of accessing the drive, a district court ruled. The court rejected the plaintiff's argument that compensable loss was established by an expert's report estimating the cost of examining third-party computers to which the plaintiff's files were allegedly copied in order to delete any unauthorized copies, commenting that such a construction of the CFAA would expand its scope to reach "a garden variety case of conversion, for which state law provides an adequate remedy."

Doyle v. Taylor, 2010 U.S. Dist. LEXIS 51058 (E.D. Wash. May 24, 2010).

Editor's Note: An interesting issue raised by the defendant but not addressed by the court is whether a thumb drive is a "computer" within the meaning of the CFAA definition: "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand-held calculator, or other similar device." The defendant argued that a "thumb drive" is not a computer because it only stores data and does not process it, and it does not have any communications capabilities. Plaintiff's Memorandum in Support of Summary Judgment, at 14-15.

PRIVACY

No Fourth Amendment Violation in Government Employer Review of Employee Text Messages

A municipality did not violate an employee's privacy rights when it reviewed text messages on an employer-supplied pager in order to determine whether it was providing sufficient character limits to its employees under its contract with the wireless services provider, the U.S. Supreme Court ruled. In a unanimous opinion, the Court found that the municipality was motivated by a non-investigatory, legitimate, work-related purpose, and that the warrantless search was reasonably related to the employer's objective and was not excessive.

City of Ontario, California v. Quon, 2010 U.S. LEXIS 4972 (U.S. June 17, 2010).

Editor's Note: This opinion is further discussed in this Proskauer Client Alert - U.S. Supreme Court Unanimously Overturns Ninth Circuit.

Warrant Required for Delayed Search of Laptop Seized at Border

While the search of a laptop computer at a border crossing did not require a search warrant, one of two subsequent warrantless searches of the laptop after it was seized by law enforcement officials violated the Fourth Amendment, a district court ruled. The court concluded that the discovery of a single image of child pornography during the border search did not destroy the laptop owner's reasonable expection of privacy in the remaining contents of the laptop that were not viewed during the border search. A second search of the laptop a week later, the court found, was justified as an "extended border search" supported by the law enforcement officials' "reasonable suspicion" that the laptop contained child pornography. A third search conducted some months later, which yielded thousands of images of child pornography, required a warrant, the court concluded, because of the "time and distance" between the search and the border.

United States v. Hanson, No. CR 09-00946 JSW (N.D. Cal. June 2, 3010) (unpublished)

No Fourth Amendment Violation in ISP Scanning of User E-Mail, and Reporting of Suspected Child Pornography in Compliance with Law

An Internet service provider that scanned user e-mail in order to screen out images containing child pornography, and reported suspected images in compliance with federal law, was not acting as an agent of law enforcement for Fourth Amendment purposes, the U.S. Court of Appeals for the Fourth Circuit ruled. The federal law in question, 42 U.S.C. § 13032(b)(1) (amended and now codified at 18 U.S.C. § 2258A), required an ISP that obtained knowledge of facts or circumstances indicating a violation of federal child pornography laws to report that information to a cyber tip line. The court rejected the characterization of the ISP as an agent of law enforcement, noting that the federal law did not require ISPs to screen transmissions on their systems, nor require them to actively seek out such content. The court also rejected the argument that the statutory penalties for noncompliance, coupled with the provision providing immunity to service providers from civil liability for actions taken in good faith to comply with the reporting requirement, rendered the ISP an agent of law enforcement.

United States v. Richardson, 607 F.3d 357 (4th Cir. June 11, 2010)

Editor's Note: The court remarked that the immunity provision protected service providers from liability for compliance with the reporting requirement, but the immunity provision did not extend to investigation of violations of child pornography laws.

No Fourth Amendment Violation in Government Administrative Subpoena to ISP for Subscriber Information

An administrative subpoena served upon a defendant's Internet service provider to obtain his subscriber information did not violate his Fourth Amendment rights, the U.S. Court of Appeals for the Fourth Circuit ruled, because the defendant had no reasonable expection of privacy in his subscriber information. The court found that there was no evidence that the defendant had a subjective expectation of privacy in his name, e-mail address, telephone number and physical address, which he had voluntarily conveyed to the provider. The court also concluded that the defendant had no objectively reasonable expectation of privacy, noting that "'[e]very federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation,'" citing United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008).

United States v. Bynum, 604 F.3d 161 (4th Cir. May 5, 2010), cert. denied (U.S. June 14, 2010)

Third-Party Civil Discovery Subpoena to Web Mail and Social Networking Providers Unenforceable under Stored Communications Act

A third-party civil discovery subpoena issued to providers of Web mail services and social networking services is unenforceable under the Stored Communications Act, a district court ruled. The court noted that the SCA prohibits a provider of an "electronic communications service" (ECS) from knowingly divulging the contents of a communication while it is in "electronic storage," and similarly prohibits a provider of a "remote communications service" (RCS) from knowingly divulging the contents of communications carried or maintained on that service. The court concluded that a Web mail provider or a social networking service that provides internal e-mail services can be both an ECS and an RCS within the meaning of the SCA, and that both unread and read mail on such services is protected from disclosure. The court also concluded that information on social network services, such as pages and comments, are protected from disclosure via third-party subpoena to the extent that access to them is limited by the user's privacy settings and they are not available to the general public.

Crispin v. Audigier Inc., 2010 U.S. Dist. LEXIS 52832 (C.D. Cal. May 26, 2010)

Editor's Note: This opinion is of particular interest for its extensive analysis of the applicability of the Stored Communications Act to relatively recent communications technologies such as Web mail and social networking sites that were not in use when the SCA was drafted.

Internet Subscriber Lacks Privacy Interest in ISP Account Information Sought by Plaintiff in Copyright Infringement Action

An Internet service subscriber lacks a privacy interest in account information sought in a subpoena served upon the subscriber's Internet service provider, a district court ruled. The subpoena was served on the ISP by the plaintiff in a multi-defendant copyright infringement action alleging unauthorized downloading of a copyrighted motion picture. The court declined to quash the subpoena in response to the subscriber's assertions that constituted a denial of the merits of the copyright infringement claim, finding that those assertions were not properly raised on a motion to quash a subpoena seeking discovery. The court also rejected the subscriber's claim that the subpoena should be quashed on the ground that it sought confidential information, finding that computer users do not have an expectation of privacy in subscriber information conveyed to a third party, i.e., the system operator, citing Guest v. Leis (6th Cir. 2001).

Worldwide Film Entertainment, LLC v. Does 1-749, 2010 U.S. Dist. LEXIS 47238 (D.D.C., May 13, 2010)

Editor's Note: The magistrate judge ruled similarly on motions filed by several other defendants in the same action seeking to quash the subpoena on the same or similar grounds, see Worldwide Film Entertainment, LLC v. Doe, 2010 U.S. Dist. LEXIS 48400 (D.D.C. May 17, 2010); 2010 U.S. Dist. LEXIS 49406 (D.D.C. May 19, 2010); 2010 U.S. Dist. LEXIS 49724 (D.D.C. May 20, 2010).

Broad Civil Discovery Order to Produce Cellphone and Computer Violated Privacy, Self-Incrimination Rights and Privileges

A civil discovery order requiring a party to produce her cellphone and computer for examination by her adversary's attorney was improper because the unlimited breadth of the order failed to protect the party's right of privacy, right against self-incrimination, and various privileges, a Florida appeals court ruled. The court noted that the there was no evidence that the party had engaged in destruction of evidence or thwarting of discovery, and that the request sought the devices themselves rather than specific relevant information that might be contained on the devices. The court also noted that the adversary had made no request to the party that she search the devices herself, in order to protect confidential documents, and that there were less intrusive means available to the adversary to obtain the same discovery without violating the party's rights and privileges.

Holland v. Barfield (Estate of Brandon Leford), 35 So. 3d 953 (Fla. Ct App. 5th Dist., May 7, 2010)

Allegations of Increased Exposure to Identity Theft Risk Insufficient to Maintain Negligence, Breach of Contract Claims

A complaint alleging negligence, breach of contract and other claims stemming from a breach in the security of personal information in the hands of a retailer was legally insufficient because the plaintiff failed to show that the loss of his personal information harmed him in a legally cognizable way, the U.S. Court of Appeals for the Ninth Circuit ruled. The court concluded, among other things, that the plaintiff's negligence claim was insufficient for failure to show actual damages. The court found that even if time or money spent on credit monitoring were sufficient to show actual damages, the plaintiff failed to provide evidence of such expenditures. The court also rejected the plaintiff's invasion of privacy claim under California law, finding that California courts have yet to extend this cause of action to accidental or negligent conduct, and further, it is not clear that an increased risk of a privacy invasion, rather than an actual privacy invasion, suffices to establish such a claim.

Ruiz v. Gap Inc., 2010 U.S. App. LEXIS 10984 (9th Cir. May 28, 2010)

Editor's Note: The ruling is discussed further on the Proskauer Privacy Law blog.

ELECTRONIC MARKETING

EU Privacy Agency Issues Opinion on Online Behavioral Advertising

The European Union's Article 29 Data Protection Working Party has issued an opinion clarifying the applicability of the EU privacy framework to online behavioral advertising. Among other things, the opinion states that placement of cookies and "similar devices" on user computers is permissible only with the "informed consent" of users and that current browser technology allows for such consent only under very limited circumstances. The opinion suggests that ad network providers should develop opt-in mechanisms requiring "affirmative action" by users to indicate willingness to receive cookies and be subject to monitoring for purposes of serving "tailored advertising," and that such monitoring be limited in time, provide for easy revocation, and offer "visible tools to be displayed where the monitoring takes place." The opinion further comments that advertising network providers should comply with EU laws requiring rights of access, rectification and retention with respect to the data collection that takes place in the context of behavioral advertising.

Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising (June 22, 2010)

No Violation of California Anti-Spam Law in Transmission of Commercial E-Mail from Multiple Domains to Bypass Spam Filters

A marketer did not violate California anti-spam laws when it sent e-mails from multiple domains in order to bypass spam filters, the California Supreme Court ruled. The plaintiff alleged that he received multiple unsolicited e-mail advertisements from a marketer with header information referencing 11 different domain names traceable to a single IP address, and further alleged that the marketer used the multiple domain names in order to reduce the chances that the recipients' ISP would identify the messages as spam and block them. The court noted that the provision at issue, California Business and Professions Code Section 17529.5, subdivision (a)(2) provides that it is unlawful to advertise in a commercial electronic mail advertisement if the advertisement “contains or is accompanied by falsified, misrepresented, or forged header information.” The court concluded that the domain names referenced in the e-mail header information "actually exist and are technically accurate, literally correct, and fully traceable" to the marketer that sent them, and therefore the e-mails did not contain misrepresented header information.

Kleffman v. Vonage Holdings Corp., 49 Cal. 4th 334 (Cal. June 21, 2010)

Editor's Note: The issue decided by the California Supreme Court was referred for decision by the U.S. Court of Appeals for the Ninth Circuit pursuant to California court rules. The ruling is further discussed on the Proskauer Privacy Law blog.

TRADEMARKS AND DOMAIN NAMES

License Language in Contract May Render Search Ad Provider Liable under ACPA for Providing Ads to Parked Domain Names

A provider of search ads to registrants of parked domain names alleged to infringe trademarks may be liable under the Anticybersquatting Consumer Protection Act as an "authorized licensee" of the registrants, a district court ruled. The court looked to the language of an exemplar of the agreement proffered by the plaintiff, under which the registrants granted the provider the "right and license to use" the domain names in order to provide the ads. The court concluded that, depending upon the terms of the actual agreements shown to have been in force with the registrants of the parked domain names, the ad provider could be liable under 15 U.S.C. §1125(d) for using the infringing domain names as the domain name registrants' "authorized licensee." The court similarly concluded that the ad provider could be liable for "trafficking" in the domain names because the statutory definition of trafficking includes, but is not limited to, sales, purchases, loans, pledges, licenses and other transfers.

Vulcan Golf, LLC v. Google Inc., 2010 U.S. Dist. LEXIS 56786 (N.D. Ill. June 6, 2010)

Credit Card Services Firms with Knowledge of Sales of Infringing Merchandise May Be Liable for Trademark Infringement

Firms that provided credit card processing services to the operator of a Web site on which counterfeit merchandise was sold may be secondarily liable for trademark infringement, a district court ruled. The court also ruled that the company that brought the Web site operator and the processing services firms together can be held secondarily liable as well. The court found that the trademark owner had alleged sufficient facts from which it could be found that each of the defendants knew or should have known that counterfeit merchandise was being sold on the Web site, an essential finding for establishing contributory infringement. The court noted, among other things, that the trademark owner alleged that the processing services firms charged higher fees for "high risk merchant accounts" that sold "replica" items, a term synonymous with counterfeit products, and the services processed charge backs from customers dissatisfied with the merchandise and thus were aware of the nature and relative low cost of the items. The court ruled that sufficient control over the infringing activity had been established with respect to the processing firms because the credit card processing services provided by them were "a necessary element for the transaction of counterfeit goods online, and were essential to sales" on the Web site. The firms “knowingly provided a "financial bridge between buyers and sellers" which enabled them to consummate transactions in infringing goods, the court found.

Gucci America, Inc. v. Frontline Processing Corp., 2010 U.S. Dist. LEXIS 62654 (E.D.N.Y. June 23, 2010)

Alleged Cybersquatter's Inclusion of Commercial Self-Promotion on Gripe Site Precludes Dismissal of Trademark and Cybersquatting Claims

A former law firm associate who registered a ".net" domain name identical to the ".com" domain name of his former employer and used the domain name to host a "gripe site" containing criticism of the firm and its employees was not entitled to dismissal of trademark infringement and cybersquatting claims, a district court ruled. With respect to the trademark infringement and dilution claims, the court concluded that the use of the law firm's name in the domain name "could conceivably cause confusion" as to affiliation with the firm, and commercial use by the former associate could be inferred from the fact that the site contained material referring to the former associate as an attorney and included a link to his professional e-mail address. The court also found with respect to the bad faith factor under the Anticybersquatting Consumer Protection Act that it could be plausibly inferred that the former associate intended to divert customers from the law firm's Web site to the gripe site in order to promote his own legal services, and to tarnish the goodwill associated with the law firm's name.

Levinson Axelrod v. Heyburn, 2010 U.S. Dist. LEXIS 43391 (D.N.J. May 3, 2010) (Unpublished)

Registration of Domain Name Prior to Trademark Filing and Registration Dates Defeats Trademark Claim

A trademark owner's claim to a domain name, asserted under the provisions of the Uniform Domain Name Dispute Resolution Policy, must fail where the trademark was neither registered nor claimed in an application filed prior to the registration of the domain name by the respondent, a UDRP panelist ruled. The panelist reasoned that Paragraph 4(a)(i) of the UDRP requires a complainant to show that the claimed domain name is identical or confusingly similar to complainant's marks. "This provision necessarily implies that Complainant's rights must predate the registration of Registrant's domain name" the panelist concluded.

See Ruling - *Arizona State Trailer Sales, Inc. d/b/a Little Dealer Little Prices RV v. World Wide RV*, No. FA1003001315658 (Nat'l Arb. Forum, May 7, 2010)

PATENTS

Supreme Court Clarifies Test for Patent-Eligible Processes

An application designed to hedge risk in the field of commodities trading is ineligible for patent protection because it is an unpatentable abstract idea, the U.S. Supreme Court ruled. While the Court upheld the ruling of the U.S. Court of Appeals for the Federal Circuit that the application was not patentable, it clarified that while the "machine or transformation" employed by the Federal Circuit is an important tool for determining whether a process is patentable, it is not the sole test. The Court did not preclude the patentability of business methods as a general proposition, although four justices, in a concurring opinion written by Justice Stevens, took the position that methods of conducting business do not constitute patentable subject matter.

Bilski v. Kappos, 2010 U.S. LEXIS 5521 (U.S. June 28, 2010)

Editor's Note: The ruling is further discussed in this Proskauer Client Alert: The Supreme Court Clarifies the Test for Patent-Eligible Processes.

COMMUNICATIONS DECENCY ACT SECTION 230

No CDA Section 230 Immunity for Claim That Service Provider Promised to "Take Care of" Defamatory Posts

A plaintiff's allegation that an employee of an online service provider promised to "take care of" defamatory material is sufficient to state a cognizable promissory estoppel claim under California law that is not barred by Section 230 of the Communications Decency Act, a state trial court judge ruled. The court concluded that a separate promise by a service provider to remove defamatory content "is not conduct of a publisher within the meaning of 230" and, therefore, it falls outside Section 230's prohibition on imposing liability on a service provider as the "publisher" of information provided by a third party. The court relied on the Ninth Circuit ruling in Barnes v. Yahoo! (9th Cir. 2009), commenting that while it was not bound by the ruling it was nevertheless "persuasive."

Scott P. v. Craigslist, Inc. (Cal. Super. Ct. San Francisco Cty June 2, 2010) (transcript of ruling)

Editor's Note: The Ninth Circuit ruling in Barnes v. Yahoo! is discussed on the Proskauer New Media and Technology Law blog.

No Dismissal under CDA Section 230 for ISP Where Good Faith Is Challenged

An Internet service provider is not entitled to dismissal of a complaint alleging various theories of liability for blocking e-mails alleged to be spam, where the plaintiff's complaint called into question whether the ISP acted in good faith pursuant to Section 230 (c)(2) of the Communications Decency Act, a district court ruled. The court noted that Section 230(c)(2) provides immunity to a provider for blocking "otherwise objectionable" material, and further noted that immunity can extend to blocking spam e-mails. But the court found that the plaintiff sufficiently alleged that the ISP blocked his e-mails in bad faith out of concern that he had not purchased a sufficient level of service to permit the sending of e-mails he was attempting to transmit. The court also declined to dismiss the complaint with respect to two spam-blocking services, on the ground that the services had failed to show that they were providers or users of an "interactive computer service" within the meaning of Section 230.

Smith v. Trusted Universal Standards in Electronic Transactions, 2010 U.S. Dist. LEXIS 43360 (D.N.J., May 4, 2010) (unpublished)

Editor's Note: The underlying facts in this case are difficult to discern, as the court itself noted in criticizing the *pro se* plaintiff's 404-page complaint. The opinion has been strongly criticized on numerous grounds, and one commentator, who indicates that he communicated with the plaintiff about the lawsuit, has suggested that the allegations of bad faith stem from a misunderstanding on the part of the plaintiff concerning the technical aspects of e-mail sending technology and industry practices.

CDA Section 230 Protects Web Site Operator from Liability for User's Defamatory Post, Despite General Statement on Web Site Concerning Accuracy of Information

A general statement on a Web site to the effect that posted information was truthful and accurate did not deprive the Web site operators of protection from liability for defamatory statements posted by third parties under Section 230 of the Communications Decency Act, a Texas appeals court ruled. The court noted that the defamatory statements were contained in a section of the Web site designated a "Guest Book," and that a reasonable person would not assume that the general statement concerning truthfulness and accuracy of information on the site applied to posts on that portion of the site. The court further found that there was no evidence that the anonymous users who posted the defamatory statements had any legal relationship with the Web site operators that would render them "information content providers" with respect to the anonymous posts. The court also rejected on the merits the plaintiffs' claim that the Web site operators' refusal to remove the defamatory posts constituted intentional infliction of emotional distress under Texas law, finding that there was no evidence that the operators left the posts on their site to intentionally or recklessly inflict injury on the plaintiffs, or that they created the "Guest Book" portion of the site in bad faith, with an intent to injure the plaintiffs.

Milo v. Martin, 311 S.W.3d 210 (Tex. Ct. App. 9th Dist. Apr. 29, 2010)

Editor's Note: Having rejected the plaintiffs' intentional infliction of emotional distress claim on the merits, the court declined to decide whether such a claim falls outside the protection of Section 230 of the CDA. The majority opinion contained a strong statement disapproving of the result of the application of Section 230, noting its "concern" that section 230 does not provide a right to request the removal of false and defamatory material, nor provide an injured party with a remedy when such information is not removed. In a concurring opinion, one judge opined that Section 230 does not preclude an action against a Web site operator for intentional infliction of emotional distress for refusing to remove defamatory material, under certain circumstances.

ELECTRONIC MARKETING

Adverse Effect for CAN-SPAM Standing Shown by Cost of Processing Spam E-Mails

An ISP that had less than 1,000 customers for its Internet access and e-mail services established standing under the federal CAN-SPAM Act with evidence that it received 200,000 spam e-mails a day, that it spent $3,000 a month in fees to process the e-mails, and that it experienced occasional network slowdowns as a result of spam traffic, a district court ruled. The court also noted that the ISP alleged that customers had complained about the specific spam e-mails at issue, that it regularly lost customers as a result of spam e-mails, and that it would realize one-third more revenue if it did not have to spend money addressing spam. The court found that the foregoing evidence was sufficient to establish standing under the Ninth Circuit's ruling in Gordon v. Virtumundo (9th Cir. 2009), which requires "some combination of operational or technical impairments and related financial costs attributable to unwanted commercial email."

Asis Internet Services v. Rausch, 2010 U.S. Dist. LEXIS 42952 (N.D. Cal. May 3, 2010)

Editor's Note: The plaintiff, Asis Internet Services, has brought numerous actions under the federal CAN-SPAM Act, with mixed results on the issue of standing. In Asis Internet v. Optin Global, 2008 U.S. Dist. LEXIS 34959 (N.D. Cal. Mar. 27, 2008), a different judge in the Northern District of California concluded that Asis lacked standing under the CAN-SPAM Act because it had not shown sufficient adverse effect as a result of the e-mails in question, a conclusion that was affirmed on appeal, see Asis Internet v. Azoogle, 2009 U.S. App. LEXIS 26232 (9th Cir. Cal., Dec. 2, 2009). In a ruling issued this month on remand in that case, the court awarded Azoogle, the prevailing defendant, over $800,000 in attorney fees. The court reasoned that although Asis may have reasonably believed when it instituted the multi-defendant lawsuit in 2005 that it could establish standing, because the law on the issue of standing was unclear prior to the Ninth Circuit ruling in Gordon v. Virtumundo in 2009, Asis acted unreasonably in pursuing claims against the prevailing defendant Azoogle because Asis persisted in litigating against Azoogle after it became clear that Asis could not establish that Azoogle had "sent or procured" the spam e-mails in question. Asis Internet v. Optin Global, 2010 U.S. Dist. LEXIS 57825 (N.D. Cal. May 19, 2010). See also Asis Internet Services v. Member Source Media LLC, 2010 U.S. Dist. LEXIS 7055 (N.D. Cal. Jan. 28, 2010) (dismissing CAN-SPAM claims for lack of standing).

TRADE SECRETS

Software User Does Not Acquire Knowledge of Trade Secrets Embodied in Source Code

A user of software containing source code misappropriated by the software developer from a competitor does not thereby acquire the requisite knowledge of the trade secrets embodied in the source code so as to violate the California Uniform Trade Secrets Act, a California appeals court ruled. The court held that the execution of software object code did not impart knowledge to the user of the trade secrets and therefore the user did not acquire, use or disclose the trade secrets within the meaning of the CUTSA. The court referenced "strong considerations of public policy," commenting that if running executable code was deemed to constitute a "use" of trade secrets embodied in the software, "then every purchaser of software would be exposed to liability if it were later alleged that the software was based in part upon purloined source code. This risk could be expected to inhibit software sales and discourage innovation to an extent far beyond the intentions and purpose of CUTSA."

Silvaco Data Systems v. Intel Corp., 2010 Cal. App. LEXIS 771 (Cal. Ct. App. 6th Dist. Apr. 29, 2010, as modified May 27, 2010)

Printouts of Policyholder Database Files Not Protectable as Trade Secrets

Policyholder information that was contained on printouts made from an insurance company electronic database by departing insurance agents was not protected under Connecticut trade secret law because the information was readily obtainable from physical policyholder files retained by the agents, a district court ruled. The U.S. Court of Appeals for the Second Circuit noted that, under Connecticut trade secret law, information claimed as a trade secret must not be "readily ascertainable by proper means" from another source, but the information on the printouts was identical to the information that was readily ascertainable from the policyholder files. Because the insurance company had failed to establish in the district court that the departing agents were not entitled to take the physical policyholder files and utilize the information contained within them, the company's trade secret claim necessarily failed with respect to the printouts as well.

Nationwide Mutual Insurance Co. v. Mortensen, 606 F.3d 22 (2d Cir. May 11, 2010)

ELECTRONIC RECORDS

Electronic Signatures on Utah Nomination Petitions Ruled Valid

Under Utah law, electronic signatures used to execute petitions to nominate independent political candidates are valid, the Utah Supreme Court ruled. The court first looked to the general provisions of the Utah Code, which broadly defines a "signature" as including a “name, mark, or sign written with the intent to authenticate any instrument or writing,” and further specifies that a "writing" includes “printing,” “handwriting,” and “information stored in an electronic or other medium if the information is retrievable in a perceivable format.” The court also concluded that the Utah enactment of the Uniform Electronic Transactions Act applies to the Utah Election Code, and noted that the UETA provides that “[i]f a law requires a signature, an electronic signature satisfies the law.”

Anderson v. Bell, 2010 UT 47 (Utah June 22, 2010)

JURISDICTION

Second Circuit Refers Question on Situs of Copyright Injury under New York Long-Arm Statute to New York Court of Appeals

The U.S. Court of Appeals for the Second Circuit has certfied a question concerning the applicability of the New York long-arm statute to online copyright infringement to the New York State Court of Appeals. At issue is the application of N.Y.C.P.L.R. § 302(a)(3)(ii), which allows for jurisdiction over an out-of-state defendant with no contacts with New York, if, among other things, the defendant is alleged to have committed a tortious act outside the State that caused, and reasonably should have been expected by the putative defendant to cause, injury to a person or property within the State. The copyright owner contends that for purposes of assessing jurisdiction in a copyright infringement case, the injury occurs where the copyright owner is located, while the defendant contends that the situs of any injury suffered is the location of the infringer. In certifying the issue, the court commented that while the plaintiff did not argue that the fact that the injury occurred via the Internet affects the analysis of the jurisdiction issue, "we recognize that this factor may be relevant to the considerations underlying the definition of the situs of injury due to the speed and ease with which the Internet may allow out of state actions to cause injury to copyright holders resident in New York."

Penguin Group (USA), Inc. v. American Buddha, 2010 U.S. App. LEXIS 12162 (2d Cir. June 15, 2010)

DEVELOPMENTS OF NOTE

Washington Supreme Court Upholds Library Online Content Filtering Policy against First Amendment Challenge

Bradburn v. North Central Regional Library District (Wash. May 6, 2010) (on certification of question from United States District Court)

District Court Refuses to Set Aside Jury Verdict in The SCO Group v. Novell Dispute over Ownership of UNIX Source Code

Blog Post

FTC Rejects Application for Proposed COPPA Safe Harbor Program

Press Release

Canadian Court Rules Use of Competitor Keywords in Online Advertising Not Misleading

Private Career Training Institutions Agency v. Vancouver Career College (Burnaby), Inc., (British Columbia Supreme Court May 28, 2010)

Google Voluntarily Dismisses Action Seeking Declaratory Judgment on Linking to Copyrighted Content

Blog Post

Twitter Settles FTC Charges That It Failed to Protect Consumer Privacy

Press Release

Senate Committee Approves Legislation Aimed at Web Loyalty Programs

Restore Online Shoppers' Confidence Act, S.3386

FTC Permanently Shuts Down Notorious Rogue Internet Service Provider

Press Release

Related Professionals

- **Jeffrey D. Neuburger**
  Partner

- **Robert E. Freeman**
  Partner
- **Daryn A. Grossman**
  Partner