Proskauer

New Media, Technology and the Law

May 2011

Edited by **Jeffrey D. Neuburger**

Contents

COPYRIGHT

Posting Entire News Article on Nonprofit Organization's Blog Constitutes Fair Use

The re-posting of an entire news article on the blog of a nonprofit organization is fair use as a matter of law where the purpose was to educate the public, a district court ruled. The court concluded that the nonprofit's use was transformative from the use of the current copyright holder, a copyright enforcement firm, a use which the court characterized as "nothing more than litigation-driven." Thus, the court said, the defendant's use "does not constitute a substitution for plaintiff's use." The court also found that the purpose of the news article was informational and thus the work entitled to less copyright protection than a "creative work of entertainment"; that the use of the entire article was reasonable because the purpose was to educate the public and because the factual nature of the information made it "impracticable" to cut the article or edit it down; and that no market harm was demonstrated by the plaintiff.

Righthaven LLC v. Jama and Center for Intercultural Organizing, Docket No. No. 10-cv-01322 (D. Nev. Apr. 22, 2011) Opinion

Editor's Note: Righthaven is a copyright enforcement firm that has brought hundreds of lawsuits challenging the online posting of news articles of which it is the copyright assignee, primarily in the District of Nevada on behalf of the Las Vegas Review-Journal, and more recently in the District of Colorado on behalf of the Denver Post. Earlier fair use rulings in Righthaven litigations are discussed on the Proskauer New Media and Technology Law blog.

Notice of Past Infringements on Online Photo Site Does Not Obligate Operator to Proactively Screen Site

An online photo-sharing site does not have a duty to search its site for material that infringes an artist's works, even if it has received past notices of infringement of the same works from the artist, a district court ruled. The court rejected the artist's argument that her previous takedown notices gave the site actual or apparent knowledge of other infringements of her works on the site. The court concluded that imposing such a duty on the site would impermissibly shift the burden of policying copyright infringement from rightsholders to the site. In declining to impose a duty to screen on the site, the court relied on Viacom International Inc. v. YouTube Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010), and UMG Recordings Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099 (C.D. Cal. 2009)

Wolk v. Kodak Imaging Network Inc. (S.D.N.Y. Mar. 17, 2011) Opinion

Mobile Carriers Not Secondarily Liable for Copyright Infringement on Multimedia Messaging System

Mobile carriers are not liable for inducing infringement of copyright on their multimedia messaging system because they did not design the system with the object of promoting infringement, nor did they take any specific, affirmative steps to actively encourage or induce infringement by users of the system, a district court ruled in a copyright infringement action brought by a producer of multimedia messaging content. The court noted that it was undisputed that the system was capable of substantial lawful and unlawful uses. The court also found that the mobile carriers were not vicariously liable for infringement occurring via the system. The content owner did not allege that the carriers were capable of monitoring or controlling content transmitted by third parties on their system, the court found, nor was there any authority for requiring the to retrofit their system in order to do so.

Luvdarts LLC v. AT&T Mobility, LLC, No. 10-05442 (C.D. Cal. Mar. 17, 2011) Opinion

OTHER COPYRIGHT DEVELOPMENTS

Cable Operator Ordered to Disclose Subscriber Information for 1,200 Accounts

Providing information on over 1,200 subscribers who are alleged to have downloaded and distributed unauthorized copies of a motion picture on a P2P file-sharing network is not an undue burden on an ISP, a district court ruled, also rejecting arguments that the order infringed the subscribers' right to anonymous communication.

Call of the Wild Movie v. Does 1-1, No. 10-455; Maverick Entertainment Group Inc. v. Does 1-4, No. 10-569; Donkeyball Movie LLC v. Does 1-171, No. 10-1520 (D.D.C. Mar. 22, 2011) Opinion

Under New York Long-Arm Statute, Copyright Owner's Location is Situs of Copyright Harm from Online Infringement

Under N.Y.C.P.L.R. 302(a)(3)(ii), which provides for long-arm jurisdiction in cases involving out-of-state tortious acts that cause harm within the State, where unauthorized copies of copyrighted works are posted on Web sites outside New York, the situs of the resulting injury is the location of the copyright owner.

Penguin Group (USA) Inc. v. American Buddha, No. 7 (N.Y. Mar. 24, 2011) (responding to a question certified by the U.S. Court of Appeals for the Second Circuit) Opinion

In Four Cases, French Appellate Court Finds Google Liable for Copyright Infringement of Films Located on Video Search

The rulings were issued on March 21, 2011, by the Paris Court of Appeal, in Google Inc. v. Bac Films, The Factory; Google Inc. v. Compagnie des phares et balises; Google Inc. v. Bac Films, The Factory, Canal+; and Google Inc. v. Les Films de la Croisade, Goatworks Films. Blog

Google Books Settlement Would Usurp Congressional Role in Revising Copyright Law

Judge Chin found that the settlement was not "fair, adequate and reasonable," as required by the federal rules, and suggested that it might be able to be approved if it was changed to an opt-in, rather than an opt-out, settlement.

The Authors Guild v. Google, Inc., No. 05-civ-8136 (S.D.N.Y. Mar. 22, 2011) Opinion

U.S. Supreme Court Grants Review of Statute Restoring Copyright in Public Domain Works

The questions presented are whether the Progress Clause of the United States Constitution prohibits Congress from taking works out of the public domain, and whether Section 514 of the Uruguay Round Agreements Act of 1994 violates the First Amendment of the United States Constitution.

Golan v. Holder, No. 10-545 (U.S. cert. granted Mar. 24, 2011) Questions Presented

Infringement and Circumvention of Massively Multiplayer Online Video Game Yield $300,000 Damages Award

The court entered a default judgment for statutory damages for trademark and copyright infringement and circumvention of technological measures resulting from the distribution of unauthorized copies of the plaintiff's videogame.

Evony v. Holland, 2011 U.S. Dist. LEXIS 34700 (W.D. Pa. Mar. 31, 2011) Opinion

CONTRACTS

Under Arkansas Law, Insurance Law Writing Requirement Satisfied by Online Transaction

A requirement in the Arkansas law that a rejection of medical benefits in an automobile insurance policy be in writing is satisfied by an electronic form completed online, the Arkansas Supreme Court ruled. The court noted that the Arkansas enactment of the Uniform Electronic Transaction Act, Ark. Code Ann. §§ 25-32-101 to -120, provides that where "a law requires a record to be in writing, an electronic record satisfies the law." This provision, the court found, "could not be more straightforward," and could be "read harmoniously" with the requirement in the insurance law that a rejection of certain benefits must be in writing.

Barwick v. Government Employees Insurance Co., 2011 Ark. 128; 2011 Ark. LEXIS 111 (Ark., Mar. 31, 2011) Opinion

DEFAMATION AND ONLINE SPEECH

CDA Section 230 Protects Online Business Review Site from Liability for Refusing to Remove Negative Reviews

Section 230 of the Communications Decency Act protects the provider of an online business review site from liability for refusing to remove negative reviews, a district court ruled. The court stated that if the provider has taken no part in the creation of the reviews, "it is irrelevant for purposes of Section 230(c)(1) how incendiary or blatantly harassing that content may be, whether the provider has knowledge of the complained-of content, or whether it has a 'general monitoring policy' for such content." The court also ruled, however, that Section 230 does not extend to liability for the provider's own acts, including allegations that the provider removed positive reviews in order to coerce businesses to purchase advertising. While Section 230 shields service providers from liability for the removal of offensive materials, that liability is conditioned on the provider's "good faith." The court rejected the claims based upon alleged coercion, however, finding the business plaintiffs' allegations factually insufficient.

Levitt v. Yelp! Inc., No. 3:10-cv-01321-MHP (N.D. Cal. Mar. 22, 2011) Opinion

No CDA 230 Protection for Online Booksellers for Internet Sale of Book

While online booksellers are immune under Section 230 of the Communications Decency Act for defamation claims arising out of promotional material supplied by third parties and posted on the booksellers' sites, Section 230 does not extend to defamation claims arising out of the books themselves, a district court ruled. The court rejected the online booksellers' argument that Section 230 immunity applies to the online sale of books because the transaction takes place on the Internet. The court reasoned that a claim for liability for the sale of a book does not treat the bookseller "as the publisher or speaker" of third-party information within the meaning of Section 230. Nevertheless, the court concluded that the booksellers were not liable in the instant case, because the plaintiff failed to show that the booksellers had the necessary actual knowledge and reckless disregard for the truth that is constitutionally required to impose defamation liability on a distributor with respect to a “public figure.”

Parisi v. Sinclair, 2011 U.S. Dist. LEXIS 34710 (D.D.C. Mar. 31, 2011) Opinion

OTHER DEVELOPMENTS IN DEFAMATION AND ONLINE SPEECH

CDA 230 Protects Blog Owner from Liability for Third-Party Comment

The court ruled the owner of a blog is not liable for an alleged defamatory comment even if the owner viewed and approved the comment prior to publication on the blog.

Kruska v. Perverted Justice Found., 2011 U.S. Dist. LEXIS 36832 (D. Ariz. Apr. 4, 2011) Opinion

Italian Court Says Google Can Be Held Liable for Failing to Filter Libelous Search Suggestions

The attorney for a plaintiff in a defamation action brought against Google in Italy reported on his blog that a court in Milan ruled on March 31 that the search engine provider has an obligation to filter out libelous "search suggestions" that appeared when the plaintiff's name was entered as a search term.

Blog Post Order (in Italian)

COMPUTER FRAUD AND ABUSE ACT

Cost of Credit Monitoring for Victims of Data Security Breach Constitutes Loss under CFAA

The cost of providing credit monitoring for employees whose personal information was accessed as a result of unauthorized access by an inmate to a prison computer network constitutes a "loss" under the Computer Fraud and Abuse Act, the United States Court of Appeals for the First Circuit ruled. The court held that the district court properly included the cost of the credit monitoring in an order of restitution entered following the inmate's plea of guilty to 18 U.S.C. § 1030(a)(5)(B)(i), causing "loss" as a result of unauthorized computer network access. The court noted that "loss" is defined in the statute as "'any reasonable cost to any victim, including the cost of responding to an offense in addition to the cost of damage assessment, restoration of the damaged system and consequential damage like lost revenue." The court concluded that the cost of a credit check for affected employees was a reasonable cost of responding to the security breach.

United States v. Janosko, No. 10-1046 (1st Cir. Apr. 12, 2011) (Opinion by Associate Justice David Souter, sitting by designation) Opinion

Employee Violation of Employer Computer Use Policy Can Support CFAA Criminal Charge

An employee's violation of an employer's computer use policy can support a criminal charge of exceeding authorized access under the Computer Fraud and Abuse Act, a district court ruled. The appeals court reinstated charges under 18 U.S.C. § 1030(a)(4) that a former employee and his co-conspirators "knowingly and with intent to defraud," exceeded their authorized access to the employer's computer network when they copied the employer's proprietary information for the benefit of another enterprise. The court noted that the employees were subject to a computer use policy that imposed "clear and conspicuous restrictions" on both the employees' access to the computer network, that they had "fair warning that they were subjecting themselves to criminal liability." The court further commented that "as long as the employee has knowledge of the employer's limitations on that authorization, the employee "exceeds authorized access" when the employee violates those limitations. It is as simple as that."

United States v. Nosal, No. 10-10038 (9th Cir. Apr. 29, 2011) Opinion

Editor's Note: The ruling is discussed further on the Proskauer New Media and Technology Law.

PRIVACY AND DATA SECURITY

Bills to Regulate Consumer Privacy Introduced in U.S. House and Senate

Several bills aimed at regulating the collection and use of consumer personal information was introduced in Congress in April.

Senators John Kerry and John McCain are co-sponsors of the Commercial Privacy Bill of Rights Act of 2011. Among other things, the Act would require collectors of information on individuals to provide clear notice of their collection practices and the purpose for such collection. Individuals would be provided the right to opt out of certain information collection, and affirmative opt-in would be required for information defined as "sensitive." The bill would require notice to an individual of his or her ability to opt out of the collection of information for the purpose of transferring it to third parties for behavioral advertising. It also would require collectors to provide individuals either the ability to access and correct their information, or to request cessation of its use and distribution.

S. 799 (112th Cong. 1st Sess. Apr. 12, 2011) Bill Summary and Status File

Representative Cliff Stearns introduced the Consumer Privacy Protection Act. The Act contains provisions, among others, requiring covered entities to establish and make easily available a privacy policy with respect to collection, sale and disclosure of consumer information, and to notify consumers of any material change in such policy. It also would require notification to consumers that their information may be shared by third parties for a purpose unrelated to a transaction, and permit them to opt out of certain sharing of that information. The bill provides no private right of action and preempts certain state laws.

H.R. 1528 (112th Cong., 1st Sess. Apr. 13, 2011) Bill Summary and Status File

Broker and Compliance Officer Personally Fined by SEC for Customer Privacy Violations

The Securities and Exchange Commission imposed fines of $20,000 each against the former president of a broker-dealer and a former broker for their actions in transferring customer information to a new firm as the defunct firm wound down. The SEC also fined the brokerage firm's former chief compliance officer $15,000 for compliance failures and security breaches that took place at the defunct firm, some dating back to 2005. The SEC charged that the president of the firm authorized a departing broker to copy information from more than 16,000 accounts to a portable drive for transfer to the new firm, without providing prior notice to the customers and an opportunity to opt out. The SEC also noted numerous lapses in security at the defunct firm, including the theft of laptop computers and unlawful access to its e-mail system by a former employee using stolen passwords. The SEC charged that the compliance officer took no action to revise or supplement the firm's policies and procedures following these breaches.

In re Mark A. Ellis, In re Frederick O. Kraus, In re David C. Levine (SEC Apr. 7, 2011) Press Release

Editor's Note: Further discussion of the SEC enforcement action is available in this Proskauer Client Alert.

FTC Says 10-Day Limit on Online Ad Company's Cookie Opt-Out is Deceptive, Requires Five-Year Effectiveness for Opt-Out

The Federal Trade Commission settled charges of deceptive practices with an online advertising company that gave consumers the opportunity to opt out of its tracking cookies, but limited the opt-out period to ten days. According to the FTC, the ad company stated in its privacy policy that it allowed consumers to opt out of its consumer tracking activities on the Internet, but did not stated that the opt-out was effective for only ten days. After the ten-day period, the company began to drop cookies on the computers of consumers who visited the Web sites of its advertising partners. The settlement with the ad company requires it to provide consumers with the ability to opt out of its targeted advertising for a period of at least five years. The company also must destroy all identifiable user information collected as a result of the deceptive opt-out, and alert consumers who previously opted out to opt out again.

In the Matter of Chitika, Inc., FTC File No. 1023087 (Mar. 14, 2011) Press Release

FTC Consumer Privacy Settlement over Google Buzz Includes EU Safe Harbor Violations

The Federal Trade Commission settled deceptive practices charges against Google relating to the rollout of the Google Buzz social network in 2010, including charges that Google violated the substantive requirements of the EU -U.S. Safe Harbor agreement. The FTC charged that the procedures for allowing users of the Google Gmail service to opt out of Buzz were confusing, difficult to find, and ineffective. Additionally, the FTC charged that requiring users to opt out of the network rather than opt in violated statements in its previously posted privacy policy. The consent agreement bars Google from misrepresenting the privacy or confidentiality of users' personal information or misrepresenting compliance with the EU-U.S. Safe Harbor requirements or other privacy or security programs. Google also must obtain user consent prior to sharing information with third parties in a way contrary to previously posted privacy promises. Finally, the settlement further requires Google to establish and maintain a comprehensive privacy program, and it requires that for the next 20 years the company have biannual audits conducted by independent third parties to assess its privacy and data protection practices.

In re Google, Inc., FTC File No. 102 3136 (Mar. 30, 2011) Press Release

Editor's Note: Further discussion of the FTC settlement with Google is available on the Proskauer Privacy Law blog.

Decreased Value of Consumer Personal Information Resulting from Security Breach Confers Standing in Personal Injury Suit

A plaintiff whose personal data was contained in a social network service online database copied by a hacker sufficiently alleged an injury-in-fact to support Article III standing, on the theory that the value of his personal information was diminished as a result of the breach, a district court ruled. The plaintiff alleged that the security breach was enabled by the defendant's storage of user passwords in unencrypted, "plain text" form, and its failure to secure the database where the passwords were stored against well-known security vulnerabilities. The court acknowledged that the plaintiff's claim was novel, and questioned his ability to prove his damages theory, but declined to dismiss the action, citing "a paucity of controlling authority regarding the legal sufficiency of plaintiff's damages theory," and the unsettled state of the law generally regarding the unauthorized disclosure of personal information via the Internet. Despite having held that the plaintiff alleged sufficient facts to establish Article III standing, the court dismissed several of the plaintiff's substantive claims for failure to plead the particularized elements of injury, including those under the California unfair competition law and the California Penal Code.

Claridge v. Rockyou Inc. (N.D. Cal. Apr. 11, 2011) Opinion

Other Privacy Developments

FTC Finalizes Settlement with Twitter for Failure to Safeguard Consumer Personal Information

The charges arose out of lapses in the security of the social networking site's administrative accounts, which enabled hackers to gain access to both administrative and customer accounts.

In re Twitter, Inc., FTC File No. 092 3093 (Mar. 11, 2011) Press Release

No Implied Consent under SCA to Discovery of E-Mails Arises from E-Mail Account Holder's Fugitive Status

A parent who is alleged to have unlawfully taken her children to a foreign county did not thereby consent, within the meaning of the Stored Communications Act, to the disclosure of her e-mails pursuant to a civil discovery subpoena directed to her ISP, the district court ruled.

Bower v. Bower, No. 10-405 (D. Mass. Apr. 5, 2011) Opinion

No Fourth Amendment Violation in Transfer of Laptop Seized at Border for Forensic Examination

The transfer of a laptop seized at a border crossing to a facility 170 miles away for forensic examination was justified under the border search doctrine, the U.S. Court of Appeals for the Ninth Circuit ruled.

United States v. Cotterman, No. 09-10139 (9th Cir. Mar. 30, 2011) Opinion

Wiretapping in Child Custody Dispute Results in Civil Damage Award under Federal Wiretap Act

A spouse involved in a child custody dispute and her parents were assessed civil damages under the federal Wiretap Act in connection with the recording of conversations via a device hidden in a child's toy.

Lewton v. Divingnzzo (D. Neb. Feb. 18, 2011) Opinion

ELECTRONIC MARKETING

Federal CAN-SPAM Act Preempts Claim under Illinois Anti-Spam Law That E-Mail Utilizing Tracking Technology Was Misleading

A claim under the Illinois anti-spam law that the heading on a promotional e-mail was misleading because it failed to warn the recipient that the e-mail sender utilized tracking technology is preempted by the federal CAN-SPAM Act, a district court ruled. The plaintiff alleged that the heading was misleading because, if he had been warned that opening the e-mail would "provide private information" to the e-mail sender, he would not have opened it. The court noted that the CAN-SPAM Act preempts state anti-spam laws, except those that prohibit "falsity or deception" in any portion of a commercial e-mail. The court found that the plaintiff's claim was essentially one for "incomplete" or "less than comprehensive information" in the subject line, a claim that other courts have ruled is not based in "traditional tort theories" and thus is not one for "falsity or deception" within the meaning of the CAN-SPAM Act.

Martin v. CCH Inc., No. 10-3494 (N.D. Ill. Mar. 24, 2011) Opinion

CAN-SPAM Act May Be Applicable to Facebook Messages

The CAN-SPAM Act may apply to communications intended to drive users of the Facebook social network to "pages" that redirect the users to an advertiser's external Web site and also encourage them to send additional messages to other users, a district court ruled. The court refused to grant a motion to dismiss brought by an advertising and marketing company whose affiliates were alleged to have been responsible for unsolicited marketing communications directed to a user's wall, news feed, home page or inbox on the in-network message system. The court rejected the argument that the Act's definition of an "electronic mail message" includes only e-mail, finding that the plaintiffs had sufficiently pleaded that social network communications fall within the Act's definition because they are "sent to a unique electronic mail address," and because they required "some routing activity" on the part of the Facebook communications system.

Facebook Inc. v. MaxBounty Inc., No. 10-4712 (N.D. Cal. Mar. 28, 2011) Opinion

Advertiser Settles Deceptive Advertising Charges Stemming from Undisclosed Payments for Online Reviews

An advertiser that paid affiliates to post favorable reviews of its product in online articles, blog posts and other online editorial material without disclosing the arrangement agreed to pay a $250,000 fine to settle deceptive advertising charges brought by the Federal Trade Commission. The advertiser also agreed to monitor its affiliate marketers and make sure that they are not misrepresenting themselves as ordinary consumers or independent reviewers. The FTC complaint alleged that the failure to disclose the arrangement violated the agency's revised Guides Concerning the Use of Endorsements and Testimonials in Advertising.

In re Legacy Learning Systems, Inc., FTC File No. 102 3055 (Mar. 15, 2011) Press Release

TRADEMARKS AND DOMAIN NAMES

Employer May Have Violated Lanham Act, State Right of Publicity, in Impersonation of Employee on Social Media

An employer that is alleged to have posted messages impersonating an employee on her personal Facebook and Twitter pages while she was recuperating from an accident may be liable under the Lanham Act for false endorsement and under the Illinois right of publicity, a district court ruled. The employee alleged that while she was absent due to an injury, the employer authored posts and tweets promoting the employer's business that contained the employee's name and likeness and posted them to her personal accounts. The court ruled that the employee had sufficiently alleged, for purposes of a motion to dismiss the Lanham Act claim of false endorsement, that she had sustained a commercial injury based upon the employer's use of her name and likeness. The court also ruled that she had pleaded a continuing violation of her state right of publicity, on which the statute of limitations had not run when she filed her complaint.

Maremont v. Susan Fredman Design Group , N.D. Ill., No. 10-7811 (Mar. 15, 2011) Opinion

In Keyword Advertising Dispute, Ninth Circuit Says Trademark Infringement Requires More Than Initial Interest Confusion

Courts must be flexible in applying the law in the Internet context, the U.S. Court of Appeals for the Ninth Circuit emphasized in a dispute involving the use of trademark terms in keyword advertising. The appeals court extensively examined its prior rulings concerning trademark infringement in the Internet context, and concluded that the district court had incorrectly applied those rulings in issuing a preliminary injunction barring the defendant's use of the plaintiff's trademark terms in keyword advertising. In particular, the appeals court found that the district court had incorrectly applied the ruling in Brookfield Communications, Inc. v. West Coast Entertainment Corp. (9th Cir. 1999), in which the appeals court found that the use of a trademark term in a domain name resulted in actionable "initial interest confusion." The court remanded the case for reconsideration, finding that the most relevant factors for determining consumer confusion, given the nature of the alleged infringement in the case, are "(1) the strength of the mark; (2) the evidence of actual confusion; (3) the type of goods and degree of care likely to be exercised by the purchaser; and (4) the labeling and appearance of the advertisements and the surrounding context on the screen displaying the results page."

Network Automation, Inc. v. Advanced System Concepts, Inc., 10-55840 (9th Cir. March 8, 2011) Opinion

Other Trademark and Domain Name Developments

ICANN Approves .XXX Domain for Adult Content, Signs Agreement with Registrar

Domain names in the newly approved gTLD are expected to go on sale in November.ICANN Press Release

Related Professionals

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