Proskauer

New Media, Technology and the Law

September 2010

Edited by **Jeffrey D. Neuburger**

WEB ACCESSIBILITY

DEVELOPMENTS OF NOTE

COPYRIGHT

Scope of Protection

Hot News Claim in Financial Data Not Preempted by Copyright Act

A hot news misappropriation claim under New York law alleging that a licensee of financial data improperly shared the data with another business entity is not preempted by the Copyright Act, because the licensor had sufficiently alleged the "extra elements" of a hot news claim, a district court ruled. The court ruled that the licensor had sufficiently alleged in its complaint that the data was time-sensitive, that it was misappropriated while it was still time-sensitive, and that the licensor and licensee were in direct competition. The court rejected the licensee's argument that the "free-riding" element of a hot news claim was precluded by the fact that the data was licensed in return for a fee, finding that the licensee's actual use of the data was "over and above" the provisions of the license agreement and constituted a breach. The court also declined to rule that the licensor's breach of contract claim was preempted by the Copyright Act, finding that the necessary "extra element" to survive preemption was established by the licensor's promise inherent in the license agreement itself.

Banxcorp v. Costco Wholesale Corp., 2010 U.S. Dist. LEXIS 70380 (S.D.N.Y. July 13, 2010)
Download PDF

Editor's Note: This opinion is also notable for its extensive analysis of the question of copyrightability of data compilations. Compare the ruling in Agora Financial, LLC v. Samler (D. Md. June 17, 2010), finding that a hot news misappropriation claim involving the republishing of stock analysts' recommendations was preempted because the plaintiff had failed to show that the recommendations were noncopyrightable facts. The court held that a recommendation to invest in a company is not a fact, but a copyrightable original work that involves judgment and creativity.

Digital Millennium Copyright Act

Librarian of Congress Adopts New Set of DMCA Anticircumvention Exemptions

The Librarian of Congress approved a new set of exemptions from the anticircumvention provisions of the Digital Millennium Copyright Act, pursuant to the recommendation of the Register of Copyrights. The exemptions apply to persons who make noninfringing uses of six classes of works. The exemptions include an expanded category of computer programs that enable used wireless telephone handsets to connect with a wireless network (i.e., "unlocking" mobile phones), and a limited exemption for "ripping" copy-protected DVDs in order to create new, noncommercial works for criticism or comment. Another new exemption covers the modification of smartphone software in order to enable the use of software applications on the handset that are obtained from sources other than the smartphone distributor (i.e., "jailbreaking" smartphones).

Final Rule, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 75 Fed. Reg. 43825 (July 27, 2010) Download PDF

Editor's Note: The new anticircumvention exceptions are discussed further on the New Media and Technology Law blog.

Logo, Copyright Notice and Link on Web Site Constitute Copyright Management Information under DMCA

A photographer's name, logo and link on a Web site containing copyrighted photographs constitute copyright management information within the scope of the Digital Millennium Copyright Act, 17 U.S.C. § 1202, a district court ruled. The court refused to dismiss the photographer's DMCA claim against a media company alleged to have copied the photographs and authorized their display on a third party's Web site without the attribution information. The court held that under the plain language of the DMCA, the term "copyright management information" is not limited to attribution information that functions as a component of an automated copyright protection or management system.

Cable v. Agence France Presse, et al., 2010 U.S. Dist. LEXIS 73893 (N.D. Ill. July 20, 2010) Download PDF

Editor's Note: This ruling is discussed further on the Proskauer New Media & Technology Law blog.

Infringement Notices Requiring Service Provider to Reference Multiple Files Are Insufficient under Takedown Provisions of DMCA

Notices of claimed infringement that consist of multiple files that a service provider must cross-reference in order to determine the location of infringing content do not satisfy the takedown provisions of the Digital Millennium Copyright Act, a district court ruled. In evaluating several sets of notices, the court noted that one group of deficient notices consisted of a cover letter, a spreadsheet containing only the top-level URL for Web sites containing infringing content, and a DVD or hard drive containing thousands of files, all of which had to be consulted in order to determine the location of the infringing content. Requiring a service provider to examine thousands of separate files, the court concluded, would impermissibly shift the burden of locating the files from the copyright owner to the provider. In contrast, the court found that a group of notices consisting of a spreadsheet with separate columns for the infringing URL, the search terms used to locate the URL, and the location of the copyrighted work on the owner's Web site, satisfied the notification requirement.

Perfect 10, Inc. v. Google, Inc., 2010 U.S. Dist. LEXIS 75071 (C.D. Cal. July 26, 2010)
Download PDF

Editor's Note: The court also ruled that the service provider had met the threshold requirements for the safe harbors under DMCA § 512(c) for information stored at the direction of a user (for its blogging service), § 512(d) for "information location tools" (for its search engine), and § 512(b) for system caching.

Damages

Music Downloader's Due Process Rights Violated by Copyright Statutory Damages Award of $22,500 per Song

A jury award of $22,500 per song, resulting in a total award of $675,000 in statutory damages against an individual who downloaded copyrighted music files on a peer-to-peer network, violated the individual's due process rights, where he reaped no pecuniary reward from the infringement and the infringement caused the plaintiffs "minimal harm," a district court ruled. The court referenced the "plainly legitimate reasons" underlying statutory damages provisions in copyright actions, which seek to insure that copyright owners are adequately compensated where actual damages are difficult to prove, to deter copyright infringement, and to encourage licensed access to works. The court noted, however, that the U.S. Supreme Court has constrained punitive damage awards under the due process clause, and found that the jury's award was "far greater than necessary to serve the government's legitimate interests in compensating copyright owners and deterring infringement."

Sony BMG Music Entertainment v. Tenenbaum, 2010 U.S. Dist. LEXIS 68642 (D. Mass. July 9, 2010) Download PDF

CONTRACTS

Clickwrap User Agreement Bars Claims against Web Site Operator over Fraudulent Ticket Sales

A clickwrap user agreement applicable to an online ticket exchange that contained broad disclaimers of liability, including disclaimers of express and implied warranties, bars claims by users of the site based upon their purchase of fraudulent ticket purchase options, a district court ruled. The court found that terms of the agreement unambiguously barred all contract claims against the exchange that arose or were "in any way connected" with disputes between buyers and sellers on the exchange. The court also found that the express and implied warranty disclaimers in the agreement were enforceable under Illinois law because they could be construed reasonably with the other provisions of the agreement, were conspicuous and were not unconscionable. Common law fraud claims based upon statements made by the exchange's customer service representatives and executives also were rejected on the ground that they were barred by the disclaimer of express warranties.

Duffy v. The Ticket Reserve, Inc., 2010 WL 2681045 (N.D. Ill. July 6, 2010) Download PDF

Browsewrap Attorney Fee Provision between Business Parties Violates Ohio Public Policy

An attorney fee provision in a browsewrap license agreement between commercial parties is unenforceable under Ohio law, even though a jury found that the agreement had been breached, because the attorney fee provision was not the product of "free and understanding negotiation," a district court ruled. The court noted that the agreement was accessible by following a hyperlink that was displayed each time a user accessed the licensed database. The court also noted that the provision benefitted only the licensor, because it provided for an award of attorney fees only when the licensor sought to protect its rights. Enforcement of the fee provision would be against Ohio public policy regarding attorney fee provisions, the court concluded, because the agreement in which it was contained "did not require users to manifest their acceptance of--or even to view--the clause" in order to access the licensed database.

Snap-On Business Solutions, Inc. v. O'Neil & Associates, Inc., 2010 U.S. Dist. LEXIS 81502 (N.D. Ohio July 7, 2010) Download PDF

E-Mail Messages Satisfy Colorado Statute of Frauds Writing Requirement

An e-mail sent to parties involved in negotiations over the settlement of a business dispute satisfies the writing requirement in the Colorado statute of frauds, a district court ruled. The court noted that the parties agreed that the purported settlement was governed by Colorado Rev. Stat. § 38-10-112, which requires that an agreement not to be performed within a year must be in writing, because the agreement contemplated the execution of a five-year note. The court applied Colorado case law in concluding that the requirement of a writing was satisfied by the e-mail. The court further ruled, however, that the e-mail was not "signed" within the meaning of the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. § 7001(a), because the e-mail containing the purported settlement terms was not sent by the person whose name appeared as the sender but by another party who was using that person's e-mail account, and the actual sender of the e-mail averred that he transmitted it for the purpose of "consideration and voting" of the parties, and he did not have authority to bind his employer. Thus, the court concluded, the e-mail did not constitute a writing "subscribed by the party charged therewith."

Buckles Management, LLC v. InvestorDigs, LLC, 2010 U.S. Dist. LEXIS 73000 (D. Colo. July 20, 2010) Download PDF

Editor's Note: The court did not refer to the Uniform Electronic Transactions Act, which was enacted in Colorado in 2002; see Colorado Rev. Stat. 24-71.3-101, et seq. The Act contains provisions equivalent to the federal Act, including the language cited by the court in 15 U.S.C. § 7001(a).

Despite Liability Disclaimer, Domain Name Registrar May Be Liable for Social Engineering Hack of Domain Name

A domain name registrar may be liable for damages sustained by a search engine as a result of a social engineering exploit that enabled a hacker to obtain control of the search engine's domain name and redirect traffic to the hacker's political site, a district court ruled. The court noted that under controlling New York law, while a disclaimer of liability such as that in the registrar's Master Services Agreement is generally enforceable, such disclaimers may not bar liability for the registrar's wilful or grossly negligent acts, or reckless indifference to the rights of others. The court found that allegations that the hacker obtained control of the domain name because the registrar did not follow its own security procedures alleged such conduct sufficiently.

Baidu, Inc. v. Register.com, Inc., 2010 U.S. Dist. LEXIS 73905 (S.D.N.Y. July 22, 2010) Download PDF

Editor's Note: A similar analysis of a disclaimer in an online clickwrap agreement was applied in Smallwood v. NCSoft Corp., 2010 U.S. Dist. LEXIS 82484 (D. Haw. Aug. 4, 2010), where the court applied the law of Texas and Hawaii in concluding that gross negligence and fraud claims brought by an online gamer alleging that he experienced severe emotional distress from addiction to a video game were not precluded by the liability disclaimer in the game developer's online User Agreement.

Online Auction Site's User Agreement Sufficiently Proved by Production of Exemplar

The execution and terms of an online auction site's user agreement containing a forum selection clause was sufficiently proved by the production of an exemplar of the agreement, coupled with testimony of a site employee describing the process by which users registered to use the site, a state appeals court ruled. The court noted that the employee's testimony established that a user was required to register and assent to the online terms in order to use the site, and the assent was required to be confirmed by the entry of a code e-mailed to the user. The court also ruled that the user's assertion that he was not aware that the agreement contained a forum selection clause was insufficient to render the clause unenforceable.

In re eBay, Inc., 2010 Tex. App. LEXIS 5340 (Tex. Ct. App. 9th Dist. July 8, 2010)
Download PDF

Editor's Note: The court in Smallwood v. NCSoft Corp., 2010 U.S. Dist. LEXIS 82484 (D. Haw. Aug. 4, 2010) similarly rejected a challenge to the authenticity of an online user agreement proffered by a video game company, where the agreement was accompanied by a declaration of in-house counsel

COMMUNICATIONS DECENCY ACT SECTION 230

New Federal Law Limits Enforcement of Foreign Libel Judgments, Extends CDA Section 230

On August 10, the President signed H.R. 2765, the “Securing the Protection of our Enduring and Established Constitutional Heritage Act” (“SPEECH Act”), which limits the recognition and enforcement of certain foreign judgments in defamation cases. The new law prohibits both federal and state courts in the United States from recognizing and enforcing defamation judgments obtained in foreign courts that do not satisfy U.S. First Amendment and jurisdictional standards. "Defamation" is defined as including libel, slander, and "any similar claim alleging that forms of speech are false, have caused damage to reputation or emotional distress, have presented any person in a false light, or have resulted in criticism, dishonor, or condemnation of any person." The new law also extends the protections of Section 230 of the Communications Decency Act to foreign defamation judgments obtained against a "provider of an interactive computer service." Further, the new law contains procedural provisions that allow the subjects of foreign defamation judgments to remove state court enforcement actions to federal court, obtain declaratory relief in anticipation of an enforcement action, and obtain an award of attorneys' fees.

H.R. 2765, the “Securing the Protection of our Enduring and Established Constitutional Heritage Act” (“SPEECH Act”), codified at 28 U.S.C. §§ 4101-4105. Bill Summary & Status File

Web Site Owner's Assertion of CDA Section 230 in Response to Defamation Claim Not an Extortionate Threat

A Web site operator's assertion of Section 230 of the Communications Decency Act in response to a demand that allegedly defamatory third-party content be removed from its consumer complaint site does not constitute an extortionate threat under California law, a district court ruled. The court stated that it had found no authority holding that a threat to defend against a lawsuit brought by another person is extortionate. The court also noted that a threat to take legal action is not extortionate under California law unless the threat was made with knowledge that the threatened claim was false and without merit. The court took judicial notice of the fact that, to the contrary, the Web site operator has prevailed in numerous prior lawsuits seeking to impose liability for alleged defamatory statements in third-party content posted on the site.

Asia Economic Institute v. Xcentric Ventures LLC, 2:10-cv-01360-SVW-PJW (C.D. Cal. July 17, 2010) Download PDF

CDA Section 230 Protects Online Ticket Exchange from Liability for Deceptive Ticket Sales

Online ticket exchanges are protected by Section 230 of the Communications Decency Act for liability under New Jersey consumer fraud laws and regulations for deceptive offerings of tickets by third-party sellers, a state court ruled. The court rejected the argument that the exchanges were "commercial actors" and therefore not covered by Section 230, finding that the fact that the exchanges charged a service or administrative fee for the sale of the tickets did not remove them from the protection of Section 230. The court also concluded that the actions of the exchanges in the creation, development and operation of their sites did not make them "information content providers" within the meaning of Section 230. Relying on the Ninth Circuit ruling in Carafano v. Metrosplash (9th Cir. 2003), the district court found that the "essential published content" that was the subject of the lawsuit was the offer of tickets alleged to be misleading or inaccurate, and that content originated from the third-party sellers, not the exchanges.

Milgrim v. Orbitz Worldwide, LLC (N.J. Super. Ct. Ch. Div. Aug. 26, 2010) Download PDF

FIRST AMENDMENT

Identity of Anonymous Commercial Speakers Entitled to Lower Standard of Protection

Anonymous speakers who posted statements and videos disparaging a business on a competitor's Web site are entitled to a lesser degree of First Amendment protection than that applicable to political speech, the U.S. Court of Appeals for the Ninth Circuit ruled. The court found that the anonymous speech was commercial because it related "solely to the economic interests of the speaker and its audience," and it went "to the heart" of the business's commercial practices and business operations. The court further found that the " most exacting standard" applied by the trial court to unmasking anonymous speakers, derived from the Delaware Supreme Court ruling in Doe v. Cahill (Del. 2005) involving political speech, was too strict when applied to commercial speech. Nevertheless, the appeals court found that the trial court did not clearly err in its conclusions on the discoverability of identifying information in the case before it.

In re Anonymous Online Speakers, 611 F.3d 653 (9th Cir. July 12, 2010) Download PDF

Editor's Note: In a ruling filed on the same day as In Re Anonymous Online Speakers, the court in Salehoo Group Ltd v. ABC Company (E.D. Wash. July 12, 2010) quashed a subpoena seeking the identify of anonymous speakers who posted disparaging information on an Internet gripe site dedicated to criticism of the plaintiff company. Commenting that the Ninth Circuit had not yet addressed the standard applicable to unmasking anonymous speakers, the court applied the test that was articulated in Dendrite International, Inc. v. Doe No 3 (N.J. Super. Ct. App. Div. 2001), and that was subsequently modified by the Delaware court in Doe v. Cahill (Del. 2005).

Virginia Privacy Law Unconstitutional as Applied to Advocate's Online Posting of SSNs

A Virginia statute prohibiting the public disclosure of Social Security Numbers is unconstitutional as applied to a privacy advocate who posted publicly available land records containing unredacted Social Security Numbers as part of a privacy lobbying effort, the U.S. Court of Appeals for the Fourth Circuit ruled. The court held that the display of the land records containing the Social Security Numbers was First Amendment-protected speech, and that the state's attempt to restrict the truthful publication of lawfully obtained information about a matter of public significance could be justified only "when narrowly tailored to a state interest of the highest order." The court concluded that Virginia's interest in protecting privacy might be a state interest of the highest order. However, because Virginia continued to permit court clerks to make land records containing SSNs publicly available online while a process to remove them retroactively was ongoing, the court further concluded that it could not be said that the application of the statute was narrowly tailored to serve the state's interest.

Ostergren v. Cuccinelli, 2010 U.S. App. LEXIS 15254 (4th Cir. Aug. 2, 2010) Download PDF

COMPUTER CRIME STATUTES

Computer Fraud and Abuse Act

No CFAA Violation Where Software Licensor with Administrative Password Gave Server Access to Licensor's Competitor

Neither a software licensee, nor a competitor of the software licensor, violated the Computer Fraud and Abuse Act when the competitor accessed a server containing the licensor's proprietary files via a password supplied by the licensee who had been issued an administrative password by the licensor, a district court ruled. The competitor accessed the server in order to copy the licensee's data in connection with the installation of a new database system. As to the licensee, the found that the licensee's access to the server was not without authorization nor did it exceed authorized access within the meaning of the CFAA because the licensee had been given administrative access by the licensor. Although the licensor claimed that the licensee's administrative access was for a limited purpose, the court concluded that the licensee's purpose in accessing the server was irrelevant and the licensee's alleged improper purpose did not render its access unauthorized. Similarly, the court concluded that the competitor's access was not unauthorized because it utilized a password that the licensee had the authority to issue.

Atpac, Inc. v. Aptitude Solutions, 2010 U.S. Dist. LEXIS 87519 (E.D. Cal. Aug. 3, 2010) Download PDF

California Computer Crime Statute

Terms of Use Breach Not Sufficient to Trigger California Computer Crime Claim

A provider of log-in services to users of the Facebook social networking site did not access the site "without permission" under California Penal Code § 502 merely because the access constituted a breach of the site's terms of use, a district court ruled. The court found that such a broad construction of the statute would put unbridled discretion in private hands to determine the scope of the statute, which would "create a constitutionally untenable situation in which criminal penalties could be meted out on the basis of violating vague or ambiguous terms of use." The court declined to dismiss the site's § 502 claim, however, finding that to the extent that the site could prove that the service's access circumvented "technical or code-based barriers" utilized to limit or deny access to the site, then the service might be held liable under the statute.

Facebook, Inc. v. Power Ventures, Inc., 2010 U.S. Dist. LEXIS 93517 (N.D. Cal. July 20, 2010) Download PDF

Editor's Note: The ruling disposed of various other claims made by the respective parties, including the defendant's claim that Facebook violated antitrust laws by denying it access to the Facebook Web site.

PRIVACY

Bankruptcy Court Approves Destruction of Personal Information Gathered on Gay Teen Site

The judge presiding over the bankruptcy proceeding of the operator of a Web site and magazine aimed at gay teens has approved a settlement allowing the destruction of personal information of users rather than a sale to creditors as part of the bankruptcy estate. The court approved the settlement after the Federal Trade Commission raised objections to the sale, citing the Web site sign-up confirmation page, which stated that "[w]e never give your info to anybody," and a similar statement directed to subscribers of an associated print magazine. In a letter to business partners of the debtor who were asserting ownership of the data, the FTC asserted that sale of the data "would contradict the privacy statements made to original subscribers, in possible violation of" the FTC Act as an unfair or deceptive act or practice.

In re Peter Ian Cummings, No.10-144433 (Bankr. D.N.J. Aug. 3, 2010) Download PDF

Editor's Note: According to news reports, the data subsequently was destroyed pursuant to the court's order.

RiteAid Pays $1 Million Fine to Settle FTC and HHS Data Disposal Charges

Rite Aid has agreed to pay $1 million in fines to resolve allegations that it violated the Health Insurance Portability and Accountability Act by disposing of pharmaceutical bottles and prescription information into publicly accessible dumpsters near Rite Aid stores. Under the Department of Health and Human Services' resolution agreement, released on July 27, Rite Aid must implement a three-year corrective action program, which includes the adoption of revised policies and procedures concerning the disposal of sensitive health-related information, employee training programs related to the revised policies and procedures and penalties for employees who fail to comply with them. In addition to the HHS resolution agreement, Rite Aid has entered into a separate but related settlement with the FTC to resolve allegations that the company failed to live up to promises made in its privacy policy that it would protect customers' sensitive medical information. The FTC settlement will require Rite Aid to implement a comprehensive information security program and obtain independent audits of the program for twenty years.

In re RiteAid Corporation, FTC File No. 072-3121, Agreement Containing Consent Order Download PDF

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

Federal FACTA Truncation Requirements Inapplicable to E-Mailed Receipts for Online Purchases

E-mailed order confirmations are not "electronically printed" receipts subject to the truncation requirements of the Fair and Accurate Credit Transactions Act ("FACTA") amendments to the Fair Credit Reporting Act, the U.S. Court of Appeals for the Seventh Circuit ruled. FACTA prohibits the "electronic printing" of any receipt at "the point of the sale or transaction" that contains the expiration date of a consumer's credit or debit card or more than the last five digits of the credit or debit card account number. The appeals court followed the majority view among district courts that "the term 'electronically printed' reaches only those receipts that are printed on paper." The court noted that a printed receipt brings to mind "a tangible document" and "ordinarily connotes recording it on paper."

Shlahtichman v. 1-800 Contacts Inc., 2010 U.S. App. LEXIS 16484 (7th Cir. Aug. 10, 2010)

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

Wiretapping

Federal Wiretap Act Not Violated by Party's Surreptitious Recording of Conversation, Absent Intent to Commit Criminal or Tortious Act

The surreptitious recording of a conversation by a party to the conversation does not violate the federal Wiretap Act, where the party had no intent to use the recording to commit a criminal or tortious act, the U.S. Court of Appeals for the Second Circuit ruled. The court construed the one-party consent provision of 18 U.S.C. § 2511(2)(d), which forbids a person who is a party to a conversation to record it, if the "oral . . . communication is intercepted for the purpose of committing any criminal or tortious act." The court concluded that in order to violate the act, the "criminal or tortious act" must be separate and apart from the act of making the recording itself. The court further concluded that while the complaint alleged a claim for the Connecticut state law tort of intrusion on seclusion, and that the elements of that tort could be satisfied by the act of surreptitious recording, the Congressional intent behind the statute was to prevent abuse stemming from the use of recordings, not the mere act of recording. Consequently, the court reasoned, the state law tort claim could not satisfy the federal statutory requirement of intent to commit a tortious act.

Caro v. Weintraub, 2010 U.S. App. LEXIS 16755 (2d Cir. Aug. 13, 2010) Download PDF

Editor's Note: The recording took place in the context of a family dispute over administration of an estate; the recording was made by an iPhone device placed on a kitchen table. In another action involving surreptitious recording in the context of a domestic dispute, the court in Lewton v. Divingnzzo, 2010 U.S. Dist. LEXIS 89149 (D. Neb. July 28, 2010), declined to dismiss federal and Nebraska state wiretap claims against a parent involved in a child custody dispute, rejecting the argument that the prohibitions on wiretapping were categorically inapplicable to parents seeking to protect the welfare of a child. The defendant parent admitted inserting a recording device into a child's teddy bear, which recorded conversations between the child and the non-custodial parent, as well as conversations not involving the child.

Fourth Amendment

Law Enforcement Use of GPS for Prolonged Tracking Is a Search Requiring a Warrant

The prolonged use of a global-positioning device by law enforcement to surveil the movements of a suspect in a drug investigation is a search requiring a warrant, the U.S. Court of Appeals for the District of Columbia ruled. The court concluded that the surveillance was a search because it defeated the suspect's reasonable expectation of privacy in the totality of his movements over the course of a month, as distinguished from his privacy interest in a single journey from point to point in the tracked vehicle. The court commented: "A reasonable person does not expect anyone to monitor and retain a record of every time he drives his car, including his origin, route, destination, and each place he stops and how long he stays there; rather, he expects each of those movements to remain 'disconnected and anonymous.'"

U.S. v. Maynard, 2010 U.S. App. LEXIS 16417 (D.C. Cir. Aug. 6, 2010) Download PDF

ELECTRONIC MARKETING

Consumer Fraud

Public Relations Firm Settles FTC Action over Paid Online Game Reviews

A public relations firm settled a Federal Trade Commission enforcement action in which the agency alleged that the firm engaged in deceptive advertising when its employees posed as ordinary consumers posting game reviews at the online iTunes store, and it did not disclose that the reviews came from paid employees working on behalf of the developers. According to the FTC's announcement of the settlement, the firm and its sole owner are required to remove any previously posted endorsements that misrepresent the authors as independent users or ordinary consumers, and that fail to disclose a connection between the firm and its owner and the seller of a product or service. The agreement also bars the firm and its owner from misrepresenting that the user or endorser is an independent, ordinary consumer, and from making endorsement or user claims about a product or service unless they disclose any relevant connections that they have with the seller of the product or service.

In the Matter of Reverb Communications, Inc. FTC File No. 092 3199 (Aug. 2010) Download PDF

Online Marketer, E-Commerce Retailers, Settle New York Consumer Fraud Charges over Online Discount Programs

New York Attorney General Obtains $10 Million Settlement against Online Discount Programs and Participating Retailers

The New York Attorney General announced the settlement of consumer fraud complaints stemming from online discount or “Web loyalty” programs. The settlement includes a group of online retailers and service providers who offered the programs on their Web sites, as well as the third-party marketers who provided the so-called Web loyalty programs. According to the New York Attorney General's press release announcing the settlement, consumers were presented with a cash back or discount offer from the third-party marketer when completing an online transaction, but information about the terms of the offer, including the fact that their credit cards would be charged a recurring fee, "was buried in fine print and cluttered text," as was the fact that their credit card information, already provided to the retailer, would be passed through to the program provider. The Attorney General stated that because "consumers were not required to provide their financial information as part of the enrollment process, they often accepted the offer without knowing they were joining a fee-based program." Among other things, the retailers and service providers agreed to permanently end the practice of "data pass," i.e., providing customer credit card and other payment information to online discount programs.

New York Attorney General Press Release (Aug. 18, 2010) Download PDF

Editor’s Note: Online loyalty and rewards programs have been the subject of Congressional hearings. See, e.g., the May 2010 Majority Staff Report of the Senate Committe on Commerce, Science and Transportation, on "Aggressive Sales Tactics on the Internet." In June, Senator Rockefeller introduced the Restore Online Shoppers’ Confidence Act to address improper practices in online rewards programs. See also the rulings In re EasySaver Rewards Litigation and Bott v. VistaPrint USA discussed below.

Courts Split on Assent to Web Loyalty Programs

In In re Easysaver Rewards Litigation (S.D.N.Y. Aug. 13, 2010), the district court refused to dismiss a class action alleging breach of contract and fraud claims against an online retailer and the third party provider of a online rewards program. The court ruled that allegations by consumers that they were deceived into indicating assent to enrollment in the programs must be accepted as true at the motion to dismiss stage. The court concluded that the allegation that the consumers who signified assent were confused was plausible, and that the reasonableness of the consumers' "expectations about shopping on the internet and dealing with pop-up windows offering a thank you gift" could not be determined on the face of the complaint. Significantly, the court refused to consider the defendants' proffer of various documents that allegedly showed that the terms of the program had been clearly presented and that the consumers had affirmatively assented to enrollment, ruling that the consumers should have the opportunity to conduct discovery that might challenge the proffered proofs, including whether the various versions of the proffered documents correctly reflected the Web pages that were displayed to them when they undertook their transactions.

Contrary to the opinion in Easysaver, the U.S. Court of Appeals for the Fifth Circuit in Bott v. VistaPrint USA, Inc. (Aug. 23, 2010), summarily upheld the district court's dismissal of a class action suit brought by consumers whose credit cards were charged by an online Web loyalty program. In its unpublished per curiam ruling, the appeals court rejected the plaintiffs' arguments that they were "tricked into" enrolling in the programs and agreed with the lower court ruling reported at In re VistaPrint USA, Inc. (S.D. Tex. Aug. 23, 2010) that the Web pages on which the offers were made were not deceptive as a matter of law. The district court concluded that the disclosures of the program features "and other pertinent information are provided in a clear, prominent, and conspicuous manner. There are no contradictory messages, and some important disclosures are provided more than once. There is no allegation that the customer is directed to any webpages after the Shopping Essentials+ webpage. The Court's review of the webpages on which Plaintiffs' base their claims convinces the Court without reservation that, as a matter of law, the webpages are not deceptive."

In re Easysaver Rewards Litigation (S.D.N.Y. Aug. 13, 2010) Download PDF

Bott v. VistaPrint USA, Inc. (5th Cir. Aug. 23, 2010) (per curiam, unpublished), aff'ing , In re VistaPrint USA, Inc. (S.D. Tex. Aug. 23, 2010) Download PDF

Telephone Consumer Protection Act

Marketing Firm Authorship Supports Finding That Primary Purpose of Faxed Attorney Newsletter Was Advertising, Not Educational

Under the FCC's Telephone Consumer Protection Act rules, the primary purpose of a faxed attorney newsletter drafted and sent by a marketing firm was advertising rather than informational, a district court ruled. The attorney argued that the advertising content of the newsletter, consisting of 25% of a single page, was "incidental," in light of the editorial, non-advertising content comprising the remaining 75% of the newsletter. The court concluded that the attorney had provided nothing to the court to "credibly support" the argument that his primary purpose in sending the faxed newsletter was informational or educational, rather than to "build brand recognition and solicit business referrals for his law practice."

Holtzman v. Turza, 2010 U.S. Dist. LEXIS 80756 (N.D. Ill. Aug. 3, 2010) Download PDF

Editor's Note: Compare Stern v. Bluestone, 12 N.Y.3d 873, 883 N.Y.S.2d 782 (N.Y. 2009), in which the New York Court of Appeals ruled that the primary purpose of a faxed attorney newsletter that was written by the attorney who sent it was an "informational message" under the FCC's TCPA regulations, because it furnished information to attorney recipients about malpractice lawsuits, contained substantive content that varied from issue to issue, and did not contain advertisements for commercial products. The court in Stern v. Bluestone commented that while the attorney devised the reports in order to impress the recipients with his expertise and to gain referrals, such an "incidental advertisement" did not convert the newsletter into an unsolicited advertisement under the TCPA.

On Remand from Supreme Court, Second Circuit Reiterates Ruling Barring TCPA Junk Fax Class Actions under New York Law

Class actions alleging violations of the "junk fax" provisions of the federal Telephone Consumer Protection Act may not be brought under New York law, because they are barred by N.Y.C.P.L.R. 901(b), the U.S. Court of Appeals for the Second Circuit ruled. The TCPA permits private actions to enforce its provisions "if otherwise permitted by the laws or rules of a court of a state." N.Y.C.P.L.R. 901(b) prohibits class-actions suits seeking statutory damages. The case was remanded by the Supreme Court for reconsideration in light of its ruling in Shady Grove Orthopedic Associates, P.A., v. Allstate Insurance Co., 130 S. Ct. 1431 (2010), a class action brought under a provision of New York insurance law, that federal courts are not bound to follow N.Y.C.P.L.R. 901(b) under the Erie doctrine because it is preempted by Fed. R. Civ. P. 23, which authorizes class-action suits in federal courts when various criteria are met. The circuit court concluded that the ruling in Shady Grove did not preclude it from ruling that actions brought under the TCPA are barred by N.Y. C.P.L.R. 901(b), because, under the express language of the Act, Congress intended to give states "considerable power to determine which causes of action lie under the TCPA."

Holster v. Gatco, Inc., 2010 U.S. App. LEXIS 17661 (2d Cir. Aug. 24, 2010) Download PDF

Anti-Spam Laws

Ninth Circuit Applies California Supreme Court Anti-Spam Ruling, Avoids CAN-SPAM Preemption Issue

The U.S. Court of Appeals for the Ninth Circuit upheld the dismissal of an action under the California anti-spam statute, citing a ruling of the California Supreme Court on a previously certified question of controlling state law. In Kleffman v. Vonage Holdings Corp., 49 Cal. 4th 334, 232 P.3d 625 (Cal. June 21, 2010), the California Supreme Court held that 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 court found that California Business and Professions Code Section 17529.5, subdivision (a)(2), which 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," was not violated because 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. The Ninth Circuit concluded that because the California anti-spam claim was properly dismissed by the district court, it need not reach the question of whether the California statute is preempted by the federal CAN-SPAM Act.

Kleffman v. Vonage Holdings Corp., 2010 U.S. App. LEXIS 14372 (9th Cir. July 13, 2010) (unpublished) Download PDF

California Anti-Spam Law Claims Brought in Federal Court Must Satisfy Pleading Standards for Fraud Claims

A federal district court properly dismissed a claim under the California anti-spam law, California Business and Professions Code § 17529.5(a), for failure to satisfy the heightened pleading standards applicable to fraud claims under Fed. R. Civ. P. 9(b), the U.S. Court of Appeals for the Ninth Circuit ruled. The court pointed out that the provisions of the California law claimed to have been violated contain terms such as "falsified," "misleading," and "forged," which are terms common to fraud allegations, and the plaintiff's complaint repeatedly described the e-mailed advertisements in question as "fraudulent." The court also agreed with the district court that the plaintiff's claims for liquidated damages were time-barred, because such damages constitute a "penalty" under California Code of Civil Procedure § 340(a)’s one-year statute of limitations.

Hypertouch, Inc. v. Azoogle.com, Inc., 2010 U.S. App. LEXIS 14121 (9th Cir. July 9, 2010) (unpublished) Download PDF

TRADEMARKS

No Trademark Infringement in Search Engine's Sale of Trademarks to Generate Search Advertisements

A search engine's sale of trademark terms to third parties to generate search advertisements does not constitute trademark infringement, a district court ruled. The court rejected multiple federal and state, direct and secondary trademark infringement claims against the Google search engine directed against its Adwords advertising program. The court found, among other things, that such sales did not constitute direct trademark infringement, because no reasonable jury could conclude that Google's practice of auctioning trademarks as keywords creates a likelihood of confusion as to the source or origin of the trademark owner's language learning products. In finding that Google lacked any intent to confuse potential purchasers of the plaintiff's trademarked goods, the court commented that the search engine is "akin to a newspaper or magazine selling advertising space."

Rosetta Stone, Ltd v. Google, Inc., 2010 U.S. Dist. LEXIS 78098 (E.D. Va. Aug. 3, 2010)
Download PDF

JURISDICTION

Employee's Single Online Sale of Counterfeit Item to Investigator, Coupled with Employer's Business Activity, Establishes In Personam Jurisdiction under New York Law

An employee's single act of shipping a counterfeit item into New York, combined with his employer's substantial activity involving New York, supports the exercise of personal jurisdiction over the employee under N.Y. C.P.L.R. § 302(a), the U.S. Court of Appeals for the Second Circuit ruled. The court concluded that the facts in the record, viewed most favorably to the plaintiff trademark owner, established that the employee either shipped the counterfeit item himself or was responsible for its shipment. The court also found that the record established that the employer entity had made numerous sales of branded merchandise to New York customers, and that those sales could be considered in concluding that the employer entity had the requisite minimum contacts, even though those sales did not involve the trademark owner's merchandise. These additional sales could be imputed to the employee, the court concluded, because the record further established that he had shared in the employer's profits, had joint access to the employer's bank account, used revenue from the employer to pay his rent, and shared in the decision-making and execution of the purchase and sale of the branded items.

Chloe v. Queen Bee of Beverly Hills LLC, 2010 U.S. App. LEXIS 16192 (2d Cir. Aug. 5, 2010) Download PDF

Editor's Note: The opinion specifically reserves the separate question of whether the sale of a counterfeit bag to a mark owner's investigator or agent constitutes an act of trademark infringement, noting that the Second Circuit has yet to rule on the issue of "manufactured contacts."

WEB ACCESSIBILITY

Congress, Federal Agencies, Take Action on Technology Accessibility

Both Congress and the two federal agencies have recently taken action aimed at making technological advances accessible to individuals with hearing and visual limitations. In some respects, these actions overlap on various points.

On July 26, the Department of Justice published several advance notices of proposed rulemaking (ANPRM), including an ANPRM requesting comment on various issues related to extending the Department's accessibility guidelines to goods, services, programs and activities provided to the public by the twelve categories of "public accommodations" that are currently covered by its regulations. Public comments will be accepted for 180 days after the publication date of the ANPRM. The three other notices released by the Department on the same day addressed movie captioning and video description, accessibility of next-generation 9-1-1 services, and certain kinds of electronic and information technology, such as POS devices, kiosks and ATMs.

Some of the areas covered by the Department of Justice ANPRMs are also covered by H.R. 3101, the "Twentieth Century Communications and Video Accessibility Act of 2010," which was voted on favorably by the House of Representatives on July 26 and is now pending in the Senate. A companion Senate bill, S. 3304, passed the Senate on August 6. According to the statement of Rep. Edward Markey, author of the legislation, H.R. 3101 is aimed at making access to the Web easier through improved user interfaces for smart phones; requiring audible descriptions of TV on-screen action; making cable TV program guides and selection menus accessible to the visually impaired; requiring captioning of online TV; making closed captioning more accessible through improved remote controls; and requiring telecom equipment used to make calls over the Internet to be compatible with hearing aids.

The provisions of H.R. 3101 are, in turn, overlapped by an order of the Federal Communications Commission clarifying the applicability of its hearing aid compatibility rules to newer technologies. In a Further Notice of Proposed Rulemaking, the agency also seeks comment on potential revisions to its rules to ensure that individuals with hearing loss have the fullest possible access to wireless communications devices and services.

Editor's Note: Web site operators should take particular notice of the Department of Justice proposal to extend the accessibility requirements of the Americans with Disabilities Act to Web sites. The ANPRM notes the conflicting rulings of the applicability of the ADA to Web sites. Compare National Federation of the Blind v. Target Corp., 452 F. Supp. 2d 946 (N.D. Cal. 2006) ("[t]o limit the ADA to discrimination in the provision of services occurring on the premises of a public accommodation would contradict the plain language of the statute") with Access Now, Inc. v. Southwest Airlines, Co., 227 F. Supp. 2d 1312 (S.D. Fla. 2002) (Web site is only covered if it affects access to a physical place of public accommodation).

DEVELOPMENTS OF NOTE

Bureau of Industry and Security Eases Export Restrictions on Encryption Technology

Summary of Amendments

Paul Allen Technology Development Lab Files Patent Infringement Action against Multiple Technology, Electronic Commerce Companies

Interval Licensing LLC v. AOL, Inc., No. 2:2010cv01385 (W.D. Wash. complaint filed Aug. 27, 2010)

Oracle Files Patent, Copyright Action against Google Claiming Android OS Infringes Java

Oracle America, Inc. v. Google, Inc., No. 4:2010cv03561 (N.D. Cal. complaint filed Aug. 12, 2010)

Court Orders Temporary Transfer of Domain Names for Failure to Remove Copyrighted Lyrics from Web Sites

Peermusic III Ltd. v. LiveUniverse Inc., (C.D. Cal. Aug. 23, 2010)

D.C. Circuit Overturns SEC Rule Setting Fees for Access to NYSE Stock Pricing Database

Netcoalition v. SEC, 2010 U.S. App. LEXIS 16303 (D.C. Cir. Aug. 6, 2010)

Federal Court Issues Warrants Authorizing Seizure of Domain Names in Online Criminal Copyright Infringement Investigation

Press Release

Default Judgment Entered in Open Source License Enforcement Action

Press Release

World Trade Organization Rules European Union Technology Tariffs Violate Trade Agreement, Must Be Removed

WTO Information Page

Federal Prosecutor Says No Criminal Charges Will Be Brought in School Webcam Spying Case

Press Release

State Bar of Texas Discloses 63,000 Attorney E-Mail Addresses under State Sunshine Law

News Report

Multiple Lawsuits Filed over Use of "Flash Cookies" to Track Users

News Report

European Court of Justice Clarifies Trademark Law Principles Applicable to Keyword Search Advertising

Portakabin Ltd. v. Primakabin BV, No. C-558/08 (European Court of Justice July 8, 2010)

Related Professionals

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