PROSKAUER ROSE LLP

New Media, Technology and the Law

Newsletter

June - July 2009

Edited by
Jeffrey D. Neuburger

For timely news on cases and other developments, visit the New Media and Technology Law blog.

CONTENTS

COPYRIGHT

U.S. Supreme Court Denies Content Owners' Petition for Certiorari in Dispute over Deployment of Remote DVR System

The U.S. Supreme Court denied the petition for certiorari filed by content owners who challenged the planned deployment of a remote digital video recorder system ("remote DVR") by a cable television provider. The system would permit subscribers to make copies of programs and store them on servers provided by the cable television provider for later viewing. The content owners sought review of a ruling by the U.S. Court of Appeals for the Second Circuit that the deployment and use of the remote DVR system would not infringe

the copyrights of the content owners in the programming they provide to the cable television provider.

The Cartoon Network LP, LLP v. CSC Holdings, Inc. (2d Cir. 2008), cert. denied, __ U.S. __ (June 29, 2009) Download PDF

Editor's Note: The petition for certiorari is discussed further in this post on the Proskauer New Media and Technology Law blog.

User Violation of Online Terms of Use and Copying of Web Site Pages May Constitute Copyright Infringement

A developer's access to a social networking site in violation of the site's Terms of Use and the copying of Web pages in order to create an application may constitute copyright infringement, a district court ruled. The social networking site alleged that the developer created and used a user account instead of obtaining access through the site's developer program. The developer then used its application to solicit user names and passwords and utilized them to further access the social networking site, in violation of multiple terms of the ToU. The court concluded that the allegations of the complaint made out a sufficient claim of copyright infringement even though the complaint did not specify which Web pages were copied, because the plaintiff alleged copyright ownership of the entire site. The court commented that the developer "need only access and copy one page to commit copyright infringement." The court also found that the ToU prohibited any copying, even of a user's own content, by means of the type of automated methods used by the developer's application to scrape content from the site. The court concluded that the allegation that the developer accessed the site via automated means made out a claim of direct copyright infringement, while the allegation that other users utilized the developer's application to access their own profile pages made out a claim of secondary copyright infringement.

Facebook v. Power Ventures, Inc., 2009 WL 1299698 (N.D. Cal. May 11, 2009) Download PDF

Editor's Note: This case is discussed further in this post on the Proskauer New Media and Technology Law blog.

DMCA Takedown Notices to Parent Company Did Not Constitute Notice of Infringement to Subsidiary

The sending of takedown notices under the Digital Millennium Copyright Act (DMCA) to the parent company of a subsidiary did not give the subsidiary, which had a separate DMCA agent and contact information posted on its site, actual knowledge of specific infringing content on the service operated by the subsidiary, a district court held. The court ruled that because the notices were not sent to the subsidiary, the subsidiary was not disqualified from claiming the benefit of the safe harbor for infringement under DMCA § 512(c) for material stored on a network or system at the direction of a user. The court

rejected the content owner's argument that the actual notice requirement was met by the production of the notices to the subsidiary during the course of litigation, commenting that it would be "an absurd result" if a complaint or other pleading was deemed to count as a DMCA notification. The court also rejected the content owner's argument that the subsidiary should be equitably estopped from claiming the safe harbor.

Perfect 10, Inc. v. Amazon.com, Inc., 2009 WL 1334364 (C.D. Cal. May 12, 2009) Download PDF

License Fees for Internet Streaming of Music Should Be Calculated Using *In Re AOL et al.* Formula

The setting of interim fees for a blanket license for public performance of musical compositions from ASCAP by a streaming video service provided on the Internet should be calculated using the *United States v. ASCAP In re AOL et al.* standard, a district court ruled. The court rejected ASCAP's attempt to distinguish *In re AOL et al.*, finding that the premium proposed by ASCAP for allowing users the ability to select the music streamed instead of being offered pre-programmed music channels was too high. The court similarly rejected the video service provider's fee proposal on the basis that the provider calculated the interim fee based on the number of views of music videos that were "label-supplied" rather than the views of all videos in the music category, and did not take into account the relatively longer viewing time of music videos.

U.S. v. American Society of Composers, Authors and Publishers, et al., 2009 WL 1360682 (S.D.N.Y. May 13, 2009) Download PDF

Web Site Created by a Marketing Company for a Customer Is Not "Work Made for Hire" under the Copyright Act

A Web site created by a marketing company for a business customer is not a "work made for hire" under the Copyright Act, the Supreme Court of Indiana ruled. The business alleged ownership of the Web site when the marketing company which created and hosted the site took the site off-line after the business defaulted on payment to the company. The court, using the framework provided by the United States Supreme Court in *Cmty. for Creative Non-Violence v. Reid*, held that the business was not the owner of the site because, under the rules of agency law, the marketing company was an independent contractor rather than an employee of the business. The court concluded that the business was a non-exclusive licensee of the Web site, and that it breached the license when it failed to pay amounts due under its agreement with the marketing company. The court also concluded that an agreement calling for a Web site designer to fashion and program the Web site and to host the site on its own servers was not governed by Article 2 of the Uniform Commercial Code, because the "predominant thrust" of the transaction involved the provision of services, not the transfer of goods.

Conwell v. Gray Loon Outdoor Marketing Group, Inc., 2009 WL 1409477 (Ind. Sup. Ct. May 19, 2009) Download PDF

TRADEMARKS AND DOMAIN NAMES

Antitrust Challenge to Automatic Contract Renewal and Price Escalation Terms in Domain Name Registry Contract Improperly Dismissed

An antitrust complaint challenging the automatic contract renewal provision and domain name registration pricing terms in the contract between the operator of the .com domain and the Internet Corporation for Assigned Names and Numbers (ICANN) should not have been dismissed for failure to state a claim, the U.S. Court of Appeals for the Ninth Circuit ruled. The court held that the plaintiff's complaint challenging the automatic contract renewal term made out an unlawful restraint of trade claim under Section 1 of the Sherman Act because the term excludes any other potential registry operator from competition. The court also held that the complaint made out a Section 1 claim with respect to the pricing term because it alleged consumer harm in the form of higher prices that were obtained through the concerted action of the registry operator and ICANN. The court further concluded the complaint made out a Section 2 claim in alleging predatory conduct on the part of the .com operator in obtaining the contract terms aimed at monopolization of the market, and in harassing ICANN through a public media campaign, among other things.

Coalition for ICANN Transparency v. VeriSign, Inc., 2009 U.S. App. LEXIS 12514 (9th Cir. June 25, 2009) Download PDF

Distributor's Use of a Manufacturer's Trademark in a Domain Name May Cause Confusion over the Source of the Distributor's Web Site, Even If No Confusion Exists over the Source of the Goods Sold on the Site

The use of a manufacturer's trademark in a domain name used on a distributor's Web site selling the manufacturer's goods may cause a likelihood of confusion to consumers as to the source of the Web site, even though there is no confusion as to the source of the goods, a district court held. The district court ruled in response to the Ninth Circuit Court of Appeal's reversal of its prior grant of summary judgment on plaintiff's trademark infringement claims. The district court reasoned that an unsupported impression that plaintiff owns or endorses defendant's Web site was an issue of material fact requiring resolution by a fact finder.

Anlin Industries v. Burgess, 2009 U.S. Dist. LEXIS 54672 (E.D. Cal. June 26, 2009) Download PDF

False Advertising and Unfair Competition Claims for Use of Photographs on Web Site Not Precluded by Copyright License

False advertising claims brought by an employer against a former employee for the use of photographs of the employer's construction projects on the Web site of the employee's new enterprise are not precluded by the employee's purchase of a license from the photographer who created the images, a district court ruled. The court noted that the employee had managed the projects on behalf of the former employer, but the former employer claimed that the Web site of the employee's new enterprise falsely depicted the projects as its own "commercial activities." The court deemed the copyright license "irrelevant" to the Lanham Act claim, because the subject of the photographs was the basis of the false advertising claim, not the improper use of the photographs themselves.

Holt v. Schweiger Construction Co., 2009 WL 1259966 (W.D. Mo. May 15, 2009) Download PDF

Performer Entitled to Injunction where Unauthorized Web Site Claimed To Be "Official Site" and Used Singer's Stage Name in Domain Name

A performer is entitled to a preliminary injunction under Section 43(a) of the Lanham Act against her former manager restraining him from the operation of a Web site that claimed to be her "official" site and from incorporating her stage name in its domain name, a federal magistrate recommended. The court found that the performer had established a probability of success on the merits of her claim that visitors to the Web site would believe that the plaintiff has sponsored or approved the contents of the site, upon which the manager had posted nude photographs of the performer. The court noted that the plaintiff possessed a valid trademark interest in her stage name and that there was a likelihood of confusion arising from the use of her stage name in the domain name of the site and its designation as her "official" site. The court also concluded that the posting of the nude photographs would cause irreparable harm to the plaintiff, since her career would likely be damaged by the resulting unwanted public perception.

Miranda v. Guerrero, 2009 WL 1381250 (report and recommendation of magistrate May 5, 2009, approved S.D. Fla. May 15, 2009) Download PDF

Rights Holders with "Common Grievance" against Same Respondent May Consolidate UDRP Actions

Rights holders may file consolidated complaints under the ICANN Uniform Domain Name Dispute Resolution Policy (UDRP) applicable to the ".com" domain against a single respondent where they have a "common grievance" against the respondent and where it is "equitable and procedurally efficient" to consolidate the complaints, a WIPO arbitrator ruled. The arbitrator noted that the UDRP rules permit the filing of complaints with respect to multiple domain names but do not explicitly permit the consolidation of multiple complaints by multiple complainants. The arbitrator followed the criteria for consolidation

of complaints set forth in an arbitrator's ruling under the similar provisions of the UDRP applicable to the .au country code domain.

Fulham Football Club (198) Limited v. Domains by Proxy, Inc., No. D2009-0331 (WIPO May 12, 2009) Download

ONLINE CONTENT

CDA Section 230 Immunity for Blocking and Screening Offensive Content Extends to Security Software Designation of Downloadable Programs as "Adware"

A distributor of Internet security software is immune from liability under Section 230(c)(2)(B) of the Communications Decency Act for classifying downloadable software programs as "adware" and blocking their installation or interfering with their operation, the Court of Appeals for the Ninth Circuit ruled. The court held that Section 230(c)(2)(B) immunity for "good samaritan" blocking and screening of offensive material is available not only to Web site operators and Internet service providers who provide access to content, but also to developers that provide access to tools that filter content. The court concluded that the distributor of Internet security software was covered by Section 230 of the CDA because the distributor gave its customers online access to its update servers and therefore it provided "access by multiple users to a computer server" within the meaning of the statutory definition of an "interactive service provider."

Zango v. Kaspersky Lab, Inc., 2009 U.S. App. LEXIS 13682 (9th Cir. June 25, 2009) Download PDF

Web Site Operator That Solicited Third Parties to Obtain Confidential Telephone Records for Sale Is an "Information Content Provider" Not Entitled to CDA Section 230 Immunity

Section 230 of the Communications Decency Act does not provide immunity to a Web site operator that solicited third parties to obtain confidential telephone records and then sold them to customers, the Court of Appeals for the Tenth Circuit held. The appeals court upheld the lower court's grant of summary judgment on Federal Trade Commission claims that the sale of the telephone records constituted an unfair practice under the FTC Act. The court ruled that the operator was an "information content provider" within the meaning of the statutory definition of the term because, by soliciting the records and offering them for sale, the operator was "responsible" for the "development" of the information.

FTC v. Accusearch, Inc., 2009 U.S. App. LEXIS 14480 (10th Cir. June 29, 2009) Download PDF

Online Classified Ad Site Protected by CDA Section 230 from Liability Claim for Handgun Sold through Site

An online classified advertising site is protected by Section 230 of the Communications Decency Act from a claim that it is liable for injuries inflicted with a handgun sold through the site, a district court ruled. The court found that the operator of the site had shown all three elements necessary to establish the defense, i.e., that the site is an "interactive computer service," that the advertisement offering the weapon for sale was placed on the service by a third party, and that the plaintiff's complaint sought to treat the site as a "publisher" of the advertisement. The court also held that Section 230 of the CDA could be raised on a pre-answer motion to dismiss, where the elements necessary to make a finding on the issue are apparent from the face of the plaintiff's complaint.

Gibson v. Craigslist, No. 07-7735 (S.D.N.Y. June 15, 2009) Download PDF

CDA Section 230 Protects Social Networking Site from Liability for Sexual Assaults on Underage Users

A social networking site is protected under Section 230 of the Communications Decency Act from liability for sexual assaults on underage users by other users of the site, a California appeals court ruled. The court concluded that because the social networking site merely provided neutral tools which could be utilized to communicate with others, the site was not an information content provider. The court rejected the plaintiffs' argument that Section 230 of the CDA was not applicable because the plaintiffs did not seek to impose liability on account of the site's exercise of traditional editorial functions, such as editing, altering, or deciding whether to publish items or not.

Doe II v. Myspace Inc., 2009 Cal. App. Lexis 1073 (Cal. App. June 30, 2009) Download PDF

Social Networking Site That Does Not Require Users to Add Information to Profiles Protected by CDA Section 230 Immunity

A social networking Web site that merely prompted users to voluntarily supply information to their online profiles is not an "information content provider" under Section 230 of the Communications Decency Act with respect to such information, a district court held. The court held that claims against the Web site for injuries allegedly resulting from the information contained on profiles on the site were barred by Section 230 because the Web site was not an information content provider with respect to that information. The court also noted that plaintiff's argument that the Web site should be liable because it did not employ reasonable safety measures on its site to protect minors from the actions of sexual predators is foreclosed by the ruling of the U.S. Court of Appeals for the Fifth Circuit in the unrelated case, *Doe v. Myspace, Inc.*, 528 F.3d 413 (5th Cir. 2008).

Doe v. Myspace, Inc., 2009 WL 1457170 (E.D. Tex. May 22, 2009) Download PDF

Where Blogger Was the Sole Owner and Founder of Company Connected to Defamatory Posts, Both May Be Liable as Alter Egos

A company may be liable for defamatory statements on a Web site as the alter ego of the blogger who admitted posting the statements, where the plaintiff established that the blogger was the sole founder and agent of the corporation, a district court ruled. The court found that these allegations created a triable issue of fact as to whether the company and the blogger were alter egos, and whether the blogger posted the defamatory statements within the scope of his apparent authority. The court also noted that the Web site upon which the statements were posted contained the copyright symbol of the company, and the blogger was the only person able to post information on the Web site.

Saadi v. Maroun, 2009 WL 1424184 (M.D. Fla. May 20, 2009) Download PDF

No First Amendment Violation in Transfer of Teacher Who Posted Critical Comments about Coworkers on Publicly Accessible Personal Blog

The First Amendment rights of a teacher were not violated by her transfer from a supervisory position to a classroom teaching position in response to critical comments she posted about coworkers on a publicly accessible personal blog, the Court of Appeals for the Ninth Circuit ruled. The appeals court reasoned that even if some of the teacher's comments constituted a "matter of public concern" for purposes of First Amendment analysis, a school official's decision to transfer her was sustainable under the balancing test laid out in *Pickering v. Board of Education*, 391 U.S. 563 (1969). The court noted that several of the comments were "highly personal and vituperative"; that the persons to whom they referred, although they were not named, were easily identifiable; and that a number of coworkers expressed unwillingness to work with the teacher in the future. The court concluded that the school official's "reasonable prediction" that other teachers could not enter into a confidential and trusting relationship with the teacher in her supervisory function as a result of the comments met the standard set forth in *Pickering*.

Richerson v. Beckon, 08-35310 (9th Cir. June 16, 2009) (unpublished) Download PDF

ELECTRONIC DIRECT MARKETING

Telephone Consumer Protection Act Term "Call" Includes Unsolicited Text Messages

The Federal Communications Commission acted reasonably in determining that the term "call" in the Telephone Consumer Protection Act includes both voice calls and text messages, the Court of Appeals for the Ninth Circuit held. The court noted that the FCC's interpretation of the statutory term was consistent with the both the Congressional purpose in enacting the legislation and with dictionary definitions of the term. The appeals court concluded that the transmission of an unsolicited text message advertisement to a cellular

phone using an Automated Telephone Dialing System is a violation of the Telephone Consumer Protection Act. The court also held that the district court erred in holding that there was no genuine issue of material fact as to whether the equipment used to send the messages in question was capable of (1) storing or producing numbers to be called using a random or sequential number generator and (2) dialing such numbers, rather than whether the system actually stores, produces, or calls randomly or sequentially generated telephone numbers.

Satterfield v. Simon & Schuster, Inc., 2009, U.S. App. LEXIS 13197 (9th Cir. June 19, 2009) Download PDF

Attorney Newsletter Not Advertising under TCPA where Primary Purpose was Informational

An attorney's faxed newsletter containing articles and other information on the subject of attorney malpractice litigation was not actionable under the federal Telephone Consumer Protection Act because its primary purpose was informational, the New York Court of Appeals ruled. The court considered the definitional of an "informational message" set out in regulations adopted under the TCPA by the Federal Communications Commission, finding that the newsletter fit the definition 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 further noted that the FCC rule provided that a message remained "informational" even if it contained an "incidental advertisement." While the court concluded that 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.

Stern v. Bluestone, No. 87 (N.Y. June 11, 2009) Download PDF

California Anti-Spam Law Not Limited to Fraud, Therefore Preempted by Federal CAN-SPAM Act

Because the California anti-spam law is not limited to claims of common law fraud or deceit resulting from unsolicited e-mails, the law is preempted by the federal Controlling the Assault of Non-Solicited Pornography And Marketing Act (CAN-SPAM), a California trial court ruled. The court concluded that the exception to the CAN-SPAM preemption provision for state laws that prohibit "falsity or deception" preserves only those state laws that prohibit "common law fraud or deceit" in unsolicited commercial e-mails. Because the provisions of the California anti-spam statute, Cal. Bus. & Prof. Code 17529.5, extend beyond claims of fraud and deceit to encompass claims based on negligence and inadvertence, the California law is preempted to that extent by the federal Act, the court held. The court further found that since the plaintiffs could not establish any of the

traditional fraud elements with respect to the 23 e-mails alleged to have been sent by the defendants, their state law claims were preempted and were properly dismissed.

Hypertouch v. Valueclick, Inc. (Cal. Super. Ct. May 4, 2009) Download PDF

Editor's Note: As the district court noted, the question of the scope of the California anti-spam statute has been certified to the California Supreme Court by the U.S. Court of Appeals for the Ninth Circuit in *Kleffman v. Vonage Holdings Corp.*, 551 F.3d 847 (9th Cir. 2008). The California Supreme Court accepted the certified question on January 26, 2009. Note also that judges in the Northern District of California ruled differently on the preemption issue; *compare Asis Internet Services v. Consumerbargaingiveaways*, 2009 U.S. Dist. LEXIS 36523 (N.D. Cal. Apr. 17, 2009) (California anti-spam law preempted by CAN-SPAM Act) *with Asis Internet Services v. Vistaprint Ltd*, 2009 U.S. Dist. LEXIS 41384 (N.D. Cal. May 5, 2009) (California anti-spam law not preempted).

PRIVACY

Failure To Secure Client Information on Company Computer Is Cause for Employee Dismissal

An employee whose unsecured company laptop containing confidential company information was stolen after being left unattended in a car parked overnight in a parking lot was fired for cause, a federal district court ruled. The court granted summary judgment in favor of the employer on the employee's breach of contract claim, noting that the employment contract provided that an employee could be fired for failure to adhere to an employer policy, and the employer's policy required that company propriety information be protected by employees. The court noted that the employee had received a newsletter and other material from the employer that expressly cautioned employees against downloading confidential data to laptops, leaving laptops unsecured, and leaving laptops unattended overnight in places such as automobiles.

Wallinger v. BB&T Insurance Services, Inc., 2009 U.S. Dist. Lexis 50805 (W.D. Va. June 17, 2009) Download PDF

Employee's Web Mail Communications with Personal Attorney, Sent Using Employer's Computer, Not Subject to Disclosure under Employer's Electronic Communications Policy

An employee's e-mails with her attorney, sent through the employee's personal, web-based e-mail account using the employer's computer are not subject to disclosure under employer's electronic communications policy, a New Jersey appellate court ruled. The court reasoned that the policies underlying the attorney-client privilege outweigh the employer's interest in access to personal communications. The court conceded that an

employer may possess a legitimate interest in accessing an employee's personal e-mails; however, even a legitimate business interest has little force when offered as the basis for an intrusion into communications otherwise protected by the attorney-client privilege.

Stengart v. Loving Care Agency, 2009 N.J. Super. LEXIS 143 (N.J. Super. App. Div. June 26, 2009) Download PDF

Editor's Note: This opinion is also significant for the court's ruling that New Jersey ethics rules required the employer's law firm to cease reading or examining the employee's attorney-client e-mails, protect them from further revelations and notify the adverse party of its possession.

Publicity Element of Invasion of Privacy Claim Satisfied by Posting on Social Networking Site

Posting private information on a publicly accessible Internet Web site satisfies the publicity element of an invasion-of-privacy claim, the Minnesota Court of Appeals ruled. The court held that public posting on a social networking site such as MySpace satisfies the publicity element because it is "materially similar in nature to a newspaper publication or a radio broadcast" in that it is "available to the public at large." The court rejected the argument that posting on a social networking site should be treated as a private communication because webpages are not of general interest like newspaper Web sites, commenting that the relevant factor is not whether the content itself is of general interest, but "whether the content is conveyed through a medium that delivers the information directly to the public."

Yath v. Fairview Clinics, N.P., No. A08-1556 (Minn. Ct. App. June 23, 2009) Download PDF

No CFAA Violation in Record Company Access to Files Available via File-Sharing Network

Record company plaintiffs investigating the distribution of unauthorized copies of music files on a peer-to-peer file-sharing network did not violate the Computer Fraud and Abuse Act when they accessed files on a computer connected to the file-sharing network, a district court ruled. The court noted that the CFAA prohibits intentional access to a computer "without authorization." The court concluded that because the files that the plaintiffs accessed were accessible by the public, the claim that the access was unauthorized within the meaning of the CFAA was "tenuous at best." Relying on its prior ruling in *Arista Records LLC v. Doe 9*, No. 07-cv-641 (W.D. Wisc.), the court also found that the disclosure of the student'shis identity by the student's identity by his university was proper under the Family Educational Rights and Privacy Act (FERPA) because (1) the information provided constituted "directory information" and (2) because the information was provided pursuant to a court order or lawfully issued subpoena.

Loud Records LLC v. Minervini, No. 08-cv-551 (W.D. Wisc. June 3, 2009) Download PDF

No CFAA Violation in Download of Licensed Database Information and Subsequent Unauthorized Use on Commercial Web Site

Allegations that a subscriber to an electronic database of real state property information downloaded information from the database and then made it available on a commercial Web site do not make out a claim for violation of the Computer Fraud and Abuse Act, a district court ruled. The court held that there was no right to relief for such conduct under 18 U.S.C. 1030(a)(4), which prohibits unauthorized access, or exceeding authorized access, to a protected computer to obtain anything of value. The court concluded that the statute does not extend to the misuse of information that had been properly accessed, commenting that access to a computer is "without authorization" within the meaning of the statute "only when initial access is not permitted," and "exceeding authorized access" takes place "only when initial access to the computer is permitted but the access of certain information is not permitted," citing *U.S. Bioservices Corp. v. Lugo*, 595 F. Supp. 2d 1189 (D. Kan. 2009). The court also held, however, that the database owner had made out a claim for copyright infringement by alleging that the database contained not just factual information, but additional authored comment describing key attributes of the properties contained in the database.

Salestraq America, LLC v. Zyskowski, No. 2:08-CV-1368 (D. Nev. June 10, 2009)
Download PDF (1) Download PDF (2)

Wife's Access to Husband's Stored E-Mails Not an "Interception" under New York Eavesdropping Statute

A wife who continued to use the e-mail account password given to her by her husband to access his e-mail account after the commencement of a divorce proceeding did not "intercept" the e-mail within the meaning of the New York eavesdropping statute, N.Y. Penal Code 250.05, the Supreme Court of New York, Kings County, ruled. The court concluded that because the e-mails were not "in transit" from one person to another at the time the wife accessed them but were stored in the e-mail account, they had not been "intercepted." Accordingly, the court concluded that because the e-mails had not been obtained by eavesdropping, they could not be suppressed under N.Y.C.P.L.R. 4506(1) and thus could be admitted as evidence in the divorce proceeding. The court also held that the husband's commencement of a divorce proceeding did not constitute an implied revocation of permission for the wife to access his e-mail account.

Gurevich v. Gurevich, 2009 N.Y. Misc. LEXIS 1045 (N.Y. Sup. Ct. Kings Cty May 5, 2009) Download

Search of Cell Phone Contents Incident to Arrest Did Not Violate Fourth Amendment

Police officers' warrantless examination of the contents of a cell phone found on the person of an individual arrested on drug charges did not violate the Fourth Amendment because it

was "limited and reasonable," a district court held. The court noted that at the time of arrest, the officers flipped open the cell phone when it rang and observed calls identified as coming from "my house" originating at a particular telephone number. They neither answered the phone nor otherwise accessed any other information on the phone, but were able to trace the phone number to the defendant's residence via a publicly accessible Internet database. A subsequent search yielded evidence relating to the charges against the arrestee. The court concluded that the search of the cell phone was analogous to a warrantless search of "other types of personal containers found on the defendant's person that fall within [recognized exceptions]" to the warrant requirement.

U.S. v. Wurie, 2009 U.S. Dist. LEXIS 37434 (D. Mass. May 4, 2009) Download PDF

Minimum Statutory Damages under Stored Communications Act Properly Awarded for Unauthorized Access to Web Site where No Actual Damages or Profits Were Shown

A bankruptcy court's award of the minimum statutory damages under the Stored Communications Act was correct where the employee whose Web site was accessed by his employer in violation of the Act failed to show any actual damages resulting from the access or any profits on the part of the employer, a district court ruled. The court noted that the damages provision of the SCA provides that damages shall be assessed as the sum of the "actual damages suffered by the plaintiff and any profits made by the violator," but also provides for minimum damages in the amount of $1,000 per violation. The district court also affirmed the bankruptcy court's refusal to award damages for incidents of access that were deemed in a prior ruling in the case by the Ninth Circuit not to violate the SCA. See *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002).

Konop v. Hawaiian Airlines, Inc., 2009 WL 1320911 (D. Haw. May 7, 2009) Download PDF

Editor's Note: In a recent opinion, the U.S. Court of Appeals for the Fourth Circuit concluded that minimum statutory damages under the SCA should not be awarded where the plaintiff has shown neither actual damages nor profits on the part of the violator. Van Alstyne v. Electronic Scriptorium, Ltd., 560 F.3d 199 (4th Cir. 2009).

Use of Keylogger or Network Analyzer To Obtain Employee Password Information May Violate ECPA

Use of a keylogger or network analyzer to obtain an employee's personal password information may violate the Electronic Communications Privacy Act (ECPA) if found to affect interstate commerce, a district court ruled. The employee claimed that his employer used network analyzers and keyloggers to monitor employees' activities, and that the employer intercepted the employee's password and logged into his personal e-mail account without permission. The court noted that the employee's claim that his employer accessed

his stored personal e-mail does not by itself violate § 2511(1)(a) of the ECPA, but the court recognized that use of the keylogger or network analyzer may violate § 2511 if it can be shown that the monitoring "actually affected interstate commerce, " an issue better determined after discovery revealed how the monitoring actually took place.

Brahmana v. Lembo, 2009 WL 1424438 (N.D. Cal. May 20, 2009) Download PDF

UNFAIR COMPETITION

Unauthorized Use of Web Pages Does Not Constitute Cyber Terrorism under Utah Law

The unauthorized use of Web pages does not constitute "cyber terrorism" under the Utah Unfair Competition Act because the the statute is directed at attacks on intellectual property utilizing a "program, code or command" that is distinct from the intellectual property being targeted, a district court ruled. The court dismissed the Web site owner's claim under the Act, noting that that the statute defines cyber terrorism as willfully transmitting a "program, code, or command without authorization, causing a decrease in value of intellectual property." The district court refused to dismiss the Web site owner's common law claim for conversion, however, finding that a Web page has characteristics of tangible property and could thus be the subject of a conversion claim under Utah law. The court noted that like software, which has been held by the Utah Supreme Court to be tangible personal property, a Web page has a physical presence on a computer drive, causes tangible effects on computers, and can be perceived by the senses.

Margae v. Clear Link Technologies, 2009 WL 1248952 (D. Utah May 4, 2009) Download PDF

CONTRACTS

User IP Addresses Not "Personally Identifiable Information" under Software Developer's EULA

A software developer's installation of software updates onto users' computers through automatic download and the collection of the users' IP addresses did not violate the End User License Agreement (EULA) provision disclaiming collection of "personally identifiable information," a district court held. The court acknowledged that while the EULA prohibited the software developer from transmitting "personally identifiable information" from the user's computer without the user's consent, IP addresses identify computers and are not "personally identifiable information" that identify a person.

Johnson v. Microsoft, 2009 U.S. Dist. LEXIS 58174 (W.D. Wash. June 23, 2009) Download PDF

Forum Selection Clause "Reasonably Communicated" to User Who Assented to Clickwrap User Agreement

A forum selection clause was "reasonably communicated" to the user of an online auction service who assented to clickwrap terms of use containing the clause and is therefore enforceable in an action brought by users and a trade association raising antitrust and trade libel claims, a district court ruled. The court noted that it was not disputed that users were required to assent to the terms of use containing the forum selection clause in order to use the service, and that the plaintiff's own complaint asserted that he was a user of the site. Conversely, the court ruled that plaintiffs who became users of the site before the forum selection clause was included in the terms of use were not bound by the user agreement containing the clause. The court further found that the forum selection clause was mandatory, that the claims were within the scope of the clause, and the clause was neither substantively or procedurally unconscionable

Universal Grading Service v. eBay, Inc., No. 08-cv-3557 (E.D. N.Y. June 9, 2009) Download PDF

Web Site Operator's Failure to Invoke Arbitration Provision of Web Site Terms of Use in Lawsuit by User Not a Material Breach Excusing User Compliance with Other Provisions

A Web site operator's failure to invoke the arbitration provision in its Web site Terms of Use in a lawsuit brought by a user of the site does not constitute a breach of the ToU excusing the user from the application of other provisions of the ToU, a district court ruled. The court found that the operator's termination of the user's account was an immaterial breach of the ToU, since the arbitration provision was not a condition of performance and repudiation of that term of the ToU did not by itself affect the other terms of the contract.

Riggs v. Myspace, Inc., 2009 WL 1203365 (W.D. Pa. May 5, 2009) Download PDF

SOFTWARE

American Law Institute Gives Final Approval to "Principles of the Law of Software Contracts" Project

On May 19, the Proposed Final Draft of the Principles of the Law of Software Contracts was approved by the American Law Institute, subject to the discussion at the ALI annual meeting and to editorial changes. According to the ALI, approval of the draft clears the way for publication of the official text of the project. Among the principles recommended in the

approved draft are: a prohibition against the enforcement of software contract provisions that would conflict with a mandatory rule, or a purpose or policy, of federal intellectual property (§ 1.09); a requirement that license terms for "standard-form transfers of generally available software" (a term defined in the draft) be "reasonably accessible electronically" prior to the "transfer" of software (§ 2.02); and a new implied warranty of no material defects in software, which may not be disclaimed. (§ 3.05(b)).

Editor's Note: A copy of the Proposed Final Draft may be purchased from the American Law Institute, http://www.ali.org

Software Considered Computer Program and Is Taxable as Tangible Personal Property when Software Complete as Sold

Software that is complete as sold falls within the definition of a "computer program" under the Texas Tax Code and thus is taxable as tangible personal property, a Texas appeals court ruled. The court rejected the argument that the software did not fall within the definition of "computer program" because the corporation that purchased the software had made extensive modifications to the software for its use. The Court of Appeals noted that the rule's plain language does not contemplate the buyer's intended use of the program and that the corporation had purchased software that was completed and ready to use when sold.

Verizon North, Inc. v. Combs, 2009 WL 1423986 (Tex. App. Ct. Austin, May 22, 2009) Download PDF

Software Company's "General Concern" over Risk of Litigation from New Technology Development Does Not Trigger Duty To Preserve Evidence

A software company's duty to preserve evidence is not triggered by its "general concern" over the risks of potential litigation arising from the development of new technology, but only when litigation is probable and a potential claim has been identified, a district court ruled. The court noted that the software company licensed the defendants' DVD encryption technology in order to develop DVD software. When the defendants learned that the software company's product would include a feature allowing users to create copies of DVDs, they objected on the grounds that the inclusion of the feature violated the license agreement. The court held that the duty to preserve evidence arose at the time of this objection, when the software company "was on notice that litigation was probable and a potential claim was identifiable."

RealNetworks, Inc. v. DVD Copy Control Ass'n, Inc, 2009 WL 1258970 (N.D. Cal. May 5, 2009) Download PDF

CRIMINAL LAW

Use of Internet to Attract Bidders to Fraudulent Auction Qualifies Federal Defendant for "Mass Market" Sentence Enhancement

Application of the mass marketing enhancement in the U.S. Sentencing Guidelines to increase a defendant's sentence is appropriate where the defendant used the Internet to conduct large-scale advertising to attract bidders to a fraudulent online auction, the Court of Appeals for the Seventh Circuit held. The court reasoned that the use of the Internet attracts more bidders than would otherwise have been possible by other means, which potentially increases the final auction price by expanding the number of bidders. The court declined to distinguish Internet auctions from other mass-marketing frauds on the basis that there is only one victim (the winning bidder).

United States v. Heckel, 2009 U.S. App. LEXIS 13312 (7th Cir. June 22, 2009) Download PDF

"USA-Only" Shipping Legend on Export-Restricted Item on Web Site Does Not Support Jury Inference That Seller Had Knowledge of Export Control Laws

A statement on a commercial Web site selling riflescopes that "We cannot export this item outside the U.S." was not sufficient evidence from which a jury could infer that the defendant possessed knowledge that the riflescopes were subject to U.S. export control laws, the Court of Appeals for the Seventh Circuit ruled. The court reasoned that such an inference is problematic because the Web site did not provide a reason for limiting the shipping destination, and the limitation may have been displayed for reasons other than the fact that the riflescopes were "defense articles" subject to export control laws. The court noted that the limitation might have been required due to restricted territory provisions in a contract or antitrust law restrictions.

United States v. Pulungan, 2009 U.S. App. LEXIS 12736 (7th Cir. June15, 2009) Download PDF

E-mails Sent to Web Site Operator by Customers, Offered in Fraud Prosecution To Show the Operator's State of Mind, Are Not Inadmissible Hearsay

E-mails containing complaints by a Web site operator's retail customers were not inadmissible hearsay in a fraud prosecution arising from the operation of the Web site, where they were offered to show the operator's state of mind, the Court of Appeals for the Fourth Circuit held. The government introduced the e-mails during the operator's trial on wire fraud charges in connection with the operation of several online retail businesses. The court concluded that the e-mails were not hearsay because they were not offered to support

the truth of the customer complaints, but were offered to place the Web site owner's response to the e-mails in context and to demonstrate her intent, lack of mistake and notice with respect to the fraudulent transactions.

United States v. Levy, 2009 U.S. App. LEXIS 14163 (4th Cir. June 30, 2009) Download PDF

Federal Wire Fraud Conviction Based on Intrastate E-Mails Satisfies "Interstate Commerce" Requirement

A federal wire fraud conviction based on e-mails that were sent intrastate is not jurisdictionally defective because the use of the Internet for transmission of messages satisfies the interstate commerce requirement, a district court held. The court noted that the Internet "standing alone is an instrumentality of interstate commerce" and "fluctuations in internet traffic could result in the e-mail actually crossing state lines prior to reaching its final destination."

U.S. v. Fumo, 2009 U.S. Dist. LEXIS 51581 (E.D. Pa. June 17, 2009) Download PDF

Editor's Note: This opinion is also of interest for the ruling that blogging by a juror during a trial had no prejudicial effect because the postings were vague, did not address any specific facts in the trial or indicate the juror's opinion about the outcome, and, most importantly, did not result in any outside influence. In a subsequent ruling on July 7, the court also denied the defendants' motion for a new trial which was based on the fact that during the trial other jurors had knowledge of the "blogging juror's" conduct.

DEVELOPMENTS OF NOTE

U.S. Supreme Court Agrees to Review *In re Bilski* Business Method Patent Ruling

Supreme Court Docket

Craigslist Agrees to Close "Erotic Services" Section in Settlement with State AGs

Craigslist Blog

Craigslist Sues South Carolina AG over Threats to Prosecute for Prostitution; Parties Agree to Temporary Stay

Citizen Media Law Project entry

FTC Obtains Temporary Restraining Order against Alleged Deceptive Search Ads for Loan Modification Service

FTC Press Release

Technology, Media and Communications Practice Group of the Corporate Department

For more information about this practice group, contact:

Jeffrey D. Neuburger
212.969.3075 – jneuburger@proskauer.com

Daryn A. Grossman
212.969.3665 – dgrossman@proskauer.com

Kristen J. Mathews
212.969.3265 – kmathews@proskauer.com

Robert E. Freeman
212.969.3170 – rfreeman@proskauer.com