# Selected Decisions Involving Protective Orders, Confidentiality & Public Access

Kenneth J. Withers, Editor[1]
The Sedona Conference®
May 1, 2011

**Allard K. Lowenstein Int'l Human Rights Project v. Department of Homeland Security, No. 09-2225 (2d Cir. Nov. 22, 2010).** The plaintiffs in this FOIA action appealed the district court's partial grant of summary judgment to the defendants, exempting disclosure of portions of a 2004 memorandum relating to 'Operation Front Line,' a counterterrorism project related to the 2004 presidential election. The plaintiffs argued that the withheld information represents "guidelines" or in the alternative "techniques and procedures" which do not meet the criterion of Section 552 Exemption (b)(7)(E). The Court of Appeals, in affirming the district court's ruling, analyzed the "plain meaning" of the text of the Exemption and its grammatical structure and held that the phrase at issue ("if such disclosure could reasonably be expected to risk circumvention of the law") refers only to the clause referencing guidelines and not to the clause referencing techniques and procedures. Additionally, employing established dictionary definitions of the terms techniques and procedures and guidelines, The Court of Appeals concluded that guidelines refers to "resource allocation" whereas techniques and procedures refer to methods by which law enforcement personnel investigate a crime, and that an *in camera* review of the memorandum determined that the withheld portions related to techniques and procedures for law enforcement investigation.

**American Booksellers Found. for Free Expression v. Coakley, No. 10-11165-RWZ (D. Mass. Oct. 26, 2010).** The plaintiffs sought to enjoin Massachusetts from enforcing a statute amended in 2010 "which criminalizes the distribution to minors of any image or written material in electronic format that is 'harmful to minors'." The plaintiffs are distributors of "sexually frank" material in a generally accessible electronic format which makes it impracticable to control the ages of those who access the material. The plaintiffs argued that the amended statute lacks the requirement "that a sender knew that the matter was purposely disseminated to a person he *knew* to be a minor." The court granted the plaintiffs' motion for a preliminary injunction, holding that they had shown unequivocally that the amended statute violates the First

[1] The Editor is indebted to contributors Sheryle J. Gallant and Ronald J. Hedges whose work is included in this annotated bibliography.

Copyright © 2011, The Sedona Conference®
www.thesedonaconference.org

Amendment, and had met all four factors required for the issuance of a preliminary injunction, and in doing so, the court refused to "read into" the amended statute a knowledge requirement.

**American Civil Liberties Union v. Tarek ibn Ziyad Acad., 2010 WL 3926864 (D. Minn. Oct 1, 2010).** The defendants appealed a magistrate judge's ruling granting the plaintiff a protective order preventing enforcement of a confidentiality agreement against employees of the defendants. The magistrate ordered the defendants not to take legal action against current or former employees for disclosures related to the litigation. The defendants claimed that the magistrate's decision was made without affording them an opportunity to be heard and that the plaintiff wished to interview employees "secretly" and "without regard to whether they are represented by counsel." The district court, in affirming the order, concluded that current and former employees "are often fruitful sources of information" about an organization's operations and that information about the defendants' "business, finance, operations, and office procedures is public data [that] cannot be kept secret." The court admonished the defendants that attempts to enforce the confidentiality clause might require the court to draw "adverse inferences" concerning how the defendants operate.

**American Small Bus. League v. United States Small Bus. Admin., No. 09-16756 (9th Cir. Oct. 15, 2010).** The plaintiff appealed an award of summary judgment to the defendant in this FOIA action where the plaintiff had sought disclosure of certain cell phone records. The original request was fulfilled only in part, subsequent to which the plaintiff commenced this litigation to compel the SBA to disclose the remaining requested records. The district court concluded that under Section 552, the SBA had no obligation to produce the records, and that the records did not meet the definition of "records" under 552(f)(2)(b) (information "maintained for an agency by an entity under government contract, for the purposes of record management."). The Court of Appeals affirmed holding: "[i]t is undisputed" 1) that the SBA did not possess the records at the time of the request and that absent such control "the records were not 'agency records' subject to FOIA disclosure," and 2) that the records were not maintained "pursuant to a records-management contract with SBA," and therefore do not fall within the statutory definition of "records" under Section 552(f)(2)(b).

***In re* Anonymous Online Speakers, 2011 WL 61635 (9th Cir. Jan. 7, 2011).** Both parties cross-petitioned for writs of mandamus. After the district court ordered the disclosure of the identities of five anonymous online speakers who allegedly made defamatory comments about the plaintiff, three of the five speakers sought to block deposition testimony concerning their identities and the plaintiff sought to compel the disclosure of the identities of the two other speakers. The Court of Appeals denied both petitions, recognizing that anonymous speech was entitled to First Amendment protection, but that commercial speech was entitled to less protection than political speech. The Court of Appeals held the district court's order was not clearly erroneous, although the district court had erred in applying the "most exacting" standard to the discovery of anonymous commercial speech. In support of its ruling, the Court of Appeals noted that this was a discovery dispute and left to the district court "the details of fashioning the appropriate scope and procedures for disclosure." The Court of Appeals also noted that the parties entered into a tiered protective order, which is "one of the tools available … to oversee discovery of sensitive matters that implicate First Amendment rights."

Copyright © 2011 The Sedona Conference®
www.thesedonaconference.org

***In re* Application, 2010 WL 5437209 (E.D.N.Y. Dec. 23, 2010).** In connection with a criminal investigation, the Government was required to obtain a search warrant for the disclosure of "historical cell-site information" over a period of 113 days. The Government sought an order pursuant to Section 2703(d) of the Stored Communications Act. In holding that a warrant was required with a showing of probable cause, the magistrate judge rejected as binding an *order* by a district judge which reversed a similar ruling he had made. Instead, the magistrate judge relied on other decisions, and concluded that a subscriber had a reasonable expectation of privacy in "the most sensitive information about a person's life—information that goes far beyond the ordinary course of the service provider's business."

**Beaven v. United States Dep't of Justice, Nos. 08-5297/5298/5317 (6th Cir. Sept. 27, 2010).** The plaintiffs claimed the defendants permitted disclosure to inappropriate sources of a folder containing "plaintiffs' sensitive personal information" in violation of the Privacy Act and Federal Tort Claims Act. The defendants appealed the district court judgment in favor of the plaintiffs on Privacy Act claims and the plaintiffs cross-appealed from the district court's judgment for the defendants on the FTCA claim, among other things. The district court held that the defendants' actions resulted in an improper disclosure under the Privacy Act (5 U.S.C. § 552a(b) & (g)(1)(D)), that the actions were "intentional or willful" as defined by section 552a(g)(4), and that the plaintiffs were entitled to damages despite that the "final act" of leaving the folder unsecured was 'inadvertent.' At issue in the appeal was whether Section 552a(g)(4), which requires that "the agency acted in a manner that was intentional or willful," necessitated that the district court find that the *final act* resulting in improper disclosure was intentional or willful or whether it was sufficient that the court find the *entire course of conduct* that led to the improper disclosure intentional or willful (emphasis in original). The Court of Appeals concluded that a court may consider the entire course of conduct involved in an alleged improper disclosure in meeting the requirement of 552a(g)(4). The defendants' also argued that the district court abused its discretion in imposing sanctions for spoliation when it adopted a nonrebuttable adverse inference that disclosure occurred, despite the plaintiffs' failure to "establish the culpable mental state and relevance of the folder as evidence." The Court of appeals held that the district court was correct in imposing the adverse inference because it found that the 'culpable state of mind factor' is satisfied by showing that evidence was destroyed 'knowingly… or negligently' and the defendants had "intentionally destroyed the folder." The Court of Appeals based its ruling on the facts that 1) the defendants had an obligation to preserve the evidence based on notice of potential claims; 2) destroying the folder was not part of the defendants' regular business practices; 3) the defendants' assertion that the folder was not 'relevant' because it was uncertain whether it would provide 'credible evidence' was "unconvincing"; and 4) destruction of the folder 'severely compromised' the plaintiffs' case. The defendants further argued that the district court abused its discretion in its alternative ruling, *i.e.*, that the plaintiffs proved disclosure by a preponderance of the evidence. The Court of Appeals, in affirming the district court's ruling, concluded that the district court made a credibility determination in finding proof of disclosure by a preponderance. On cross-appeal, the court addressed the plaintiffs' claim that the district court erred in defining 'actual damages' under the Privacy Act to exclude plaintiff's "claims for lost time and future expenses." The Court of Appeals affirmed the district court's denial of future expenses damages but reversed the district court's judgment on 'lost time' damages concluding that the plaintiffs' invalid Federal Torts Claim Act claim did not preclude recovering damages for the plaintiffs' valid Privacy Act claims.

Copyright © 2011 The Sedona Conference®
www.thesedonaconference.org

**Blockowicz v. Williams, 630 F.3d 563 (7th Cir. 2010).** The plaintiff in this defamation action secured an injunction requiring the defendants to remove defamatory comments they allegedly posted on certain websites. One website failed to comply with the injunction and the plaintiff moved to enforce the injunction against the third party. The district court declined to enforce the injunction against the website and the Court of Appeals affirmed, holding the website (and its manager) were not "in active concert or participation" with the defendants, as required by FRCP 65(d)(2)(C). The Court of Appeals also ruled that the pre-injunction conduct of the website in entering into a "Terms of Service" agreement with the defendants and the post-injunction inactivity of the website was insufficient to show that the website aided or abetted the defendants.

***In re* The City of New York, 607 F.3d 923 (2d Cir. June 9, 2010).** In this civil rights action alleging violations of 42 U.S. C. §1983, the City of New York, the defendant, submitted a petition for a writ of mandamus directed to the U.S. District Court for the Southern District of New York. In the underlying action, **Schiller v. City of N.Y., No. 04 Civ. 7922 (S.D.N.Y. Dec. 10, 2009),** the plaintiffs sued the city alleging that were arrested, detained, and fingerprinted after demonstrating at the 2004 Republican National Convention (RNC) in violation of federal and state law. During pretrial discovery, the plaintiffs moved to compel the city to produce confidential reports created by undercover police officers who were investigating potential security threats in the months before the RNC. The city opposed the motion by asserting, among other things, that the documents were protected from disclosure by the law enforcement privilege. The district court granted the plaintiffs' motion to compel. The city, in turn, filed a petition for a writ of mandamus seeking relief from the order granting the plaintiffs' motion to compel. The Second Circuit granted the city's petition for a writ of mandamus, vacated the district court's December 10, 2009, order, and instructed the district court to deny the plaintiffs' motion to compel the production of the confidential reports. The Second Circuit based its decision on a variety of factors. First, a writ of mandamus was the only "adequate means" for the city to seek review of the district court's order and prevent irreparable harm that the city and the public would suffer from the disclosure of the reports. Second, because of the civil nature of the action, the plaintiffs' need for discovery did not yield to the law enforcement privilege. Third, the plaintiffs failed to show a compelling need for the reports. Finally, the district court erred when it found that the plaintiffs' need for the documents outweighed the public's interest in their secrecy.

**Comcast Corp. v. FCC, 600 F.3d 642 (D.C. Cir. 2010).** This action challenged an order issued by the Federal Communications Commission (FCC) requiring Comcast, which the FCC found had interfered with its customers' use of peer-to-peer networking applications, to make detailed disclosures concerning its new system for bandwidth management and progress toward implementation of the plan. Comcast complied with the order but then petitioned for review based on, among other things, a "jurisdictional challenge." At issue was whether the FCC's 'ancillary' authority under Section 4(i) of the Communications Act of 1934, permitted regulation of Comcast's network management practices. The Court of Appeals, in vacating the FCC's ruling, held that the FCC had failed to satisfy the second prong of the two-part test for the appropriate exercise of the FCC's ancillary jurisdiction. The Court of Appeals concluded that the congressional statements of policy relied upon by the FCC were insufficient to establish "statutorily mandated responsibilities," because the FCC's ancillary authority "is. . . contingent

Copyright © 2011 The Sedona Conference®

upon *specifically delegated powers under the act*," and "policy statements are just that—statements of policy. . . not delegations of regulatory authority." The Court of Appeals also rejected the Commission's attempts to support its action by reference to other provisions of the Communications Act and the Telecommunications Act of 1966 which, even though these established statutorily mandated responsibilities, did not justify the FCC's exercise of ancillary jurisdiction over Comcast's network management practices.

**In the Matter of Eastman Kodak Co.'s Application for an Order Sealing the Files in Civil Actions Against Ability Enter. Co. Ltd. & Kyocera Corp., 2010 WL 2490982 (S.D.N.Y. June 15, 2010).** Eastman Kodak Co. (Kodak) applied for permission to file certain complaints under seal or heavily redacted in this breach of contract action. Kodak argued that this relief was needed to "shield itself from counterclaims" because of private agreements to keep the terms of its license agreements confidential. The district court denied the application except with respect to redaction of the royalty rate, the appropriateness of which the court reserved for the judge assigned to the case. The district court concluded that, since the filings to be sealed or redacted do not "impact innocent third parties" but concern the parties involved and the alleged basis of the civil actions, factors central to the court's jurisdiction and the public's interest in the activities of the federal courts, the strong presumption of public access to court records should prevail.

**Electronic Priv. Info. Ctr v. Department of Homeland Security, 2011 WL 93087 (D.D.C. Jan. 12, 2011).** In this FOIA action, the plaintiff sought information pertaining to whole-body imaging technology used to screen air travelers. The defendant produced redacted documents but withheld in full certain training materials, including body images that showed "threat objects." On cross-motions for summary judgment, the district court found that the records fell within FOIA exemption "2-high," and were protected from disclosure information that is "used for predominantly internal purposes" and relates to "rules and practices for agency personnel." The court agreed with the agency's conclusion that disclosure would "significantly risk circumvention of federal regulations or statutes" by providing travelers with increased abilities to circumvent screening. The court also found that parts of images without threat objects were "inextricably intertwined" with those *with* threat objects and held that the former non-exempt information need not be disclosed.

**Johnson v. Neiman, 2010 WL 4065368 (E.D. Mo. Oct. 18, 2010).** The court granted the defendants' motion for a protective order in connection with the plaintiff's restoring and producing email on some 5,800 backup tapes. Applying FRCP 26(b)(2)(B), the court found the ESI to be not reasonably accessible because of undue burden or cost. The court also found that the plaintiff had not demonstrated good cause for production, citing the 2006 Advisory Committee Note to the rule.

**Lardner v. United States Dep't of Justice, 2010 WL 4366062 (D.C. Cir. Oct. 28, 2010).** The Department of Justice (DOJ) appealed from the district court's grant of partial summary judgment in favor of the plaintiff in this FIOA action. The district court held that the Office of Pardons (OPA) was required under Section 522 to release the names of individuals whose clemency applications were denied by the President. The Court of Appeals, in affirming the district court's grant of partial summary judgment, held that (1) the DOJ's privacy and stigma objections were "undermined" by OPA's procedures and regulations which reserve the right to release information when "investigating an applicant's suitability for clemency" and when a third

Copyright © 2011 The Sedona Conference®

party inquiry concerns 'a specific named person'; (2) the value of the information is supported by the Inspector General's Report on potential "impermissible considerations" in pardon determinations; (3) the information requested did not fall under Exemption 6 because the case precedent relied upon by the DOJ was inappropriate since it involved a request for disclosure of the contents of applications, whereas no such disclosure was sought by the plaintiff; and (4) the information requested did not fall under Exemption 7(C) because the list of names is not a law enforcement record, but a list to "inform the OPA of the President's determinations."

**McKinley v. FDIC, 2010 WL 5209337 (D.D.C. Dec. 23, 2010).** In this FOIA action, the plaintiff sent three requests for information regarding the FDIC's response to the "global financial crisis of 2008." The FDIC responded to the requests with redacted information and moved to dimiss. The court denied the FDIC's motion to dismiss on mootness grounds as the redactions remained in issue. The court found that the FDIC had not demonstrated that it had performed an adequate search for responsive information and had not demonstrated that the information withheld met any statutory exemption from disclosure. The court remanded to the FDIC.

**Mortensen v. Bresnan Communication, 2010 WL 5140454 (D. Mont. Dec. 13, 2010).** The plaintiffs in this class action asserted claims under the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act against the defendant Internet Service Provider arising out of the ISP's alleged diversion of their Internet communications to a third-party Internet advertising company, which created an "Appliance" on the ISP's network that allowed the company to profile the plaintiffs for targeted ads. The defendant moved to dismiss and the court held that the allegations of the Complaint stated a claim for "interception" under the Electronic Communications Privacy Act. However, the plaintiffs had consented to the interception through a subscriber agreement and other documents. For the same reason, the court held that the plaintiffs had no objectively reasonable expectation of privacy and dismissed an invasion of privacy claim. Turning to a claim under the Consumer Fraud and Abuse Act, the court held that the plaintiffs' damages could be aggregated to establish "damage" and that the defendant had not accessed the plaintiffs' computers "without authorization." However, the court denied the motion to dismiss, holding that there were sufficient allegations that the defendant acted in concert with the company by installing the Appliance, thus "exceeding authorized access." Finally, the court held that the allegations were sufficient to allege that the defendant had intentionally interfered with the possession of the plaintiffs' personal property and denied a motion to dismiss a trespass to chattel claim.

**National Bus. Aviation Ass'n. v. FAA, 686 F. Supp. 2d 80 (D.D.C. 2010).** In this "reverse" Freedom of Information Act (FOIA) action, the plaintiff sued to prevent release by the Federal Aviation Association (FAA) to the intervenor defendant a list of aircraft registration numbers that the plaintiff had provided to the FAA so that specific aircraft could be blocked from a program that permitted "real time or near real-time tracking" of aircraft. The plaintiff argued that the list fell under Exemption 4 (5 U.S.C. § 552 (b)(4)), which protects information that is, inter alia, "commercial or financial." In granting summary judgment in favor of the FAA, the district court held that the FAA reasonably concluded that none of the information had commercial significance, and concluded that although the list of registration numbers could be used by the recipient to obtain historical location data, the name of the owner, and the make and model of the aircraft, the plaintiff's speculation that this information "might be used to gain

Copyright © 2011 The Sedona Conference®

insight into the nature of a company's business dealings did not convert *the aircraft registration numbers themselves* into commercial information," protected by Exemption 4.

**Prison Legal News v. Executive Office, 628 F.3d 1243 (10th Cir. 2011).** In this FOIA action, the plaintiff sought disclosure of a video "depicting the aftermath of a brutal prison murder and autopsy photographs of the mutilated victim." The video and photographs had been introduced into evidence and shown in open court during the criminal trials, but then returned to the United States Attorney's Office. On appeal from a ruling of the district court that upheld the defendant's exempting the materials from disclosure, the Court of Appeals affirmed. The court concluded that the materials fell under Exemption 7(c), as these "could reasonably be expected to constitute an unwarranted invasion of personal privacy." The Court of Appeals held that the privacy interests in issue were those of the victim's family and that the use of the materials at trial was irrelevant to a waiver analysis. The court also held that any public interest in disclosure was minimal and outweighed by the family's privacy interests. The Court of Appeals did hold that the district court had erred in withholding portions of an audio track containing statements by the murderers. Nevertheless, the court affirmed nondisclosure on 7(C) grounds given the privacy interests. Finally, the court rejected the plaintiff's argument that the "public domain doctrine" compelled disclosure: Assuming the court was to recognize that doctrine, it would be inapplicable under the facts as the purpose of Exemption 7(C) remained intact. The court did not address the separate question of whether the materials had been properly removed from the public record or should have been made available for copying.

**Shropshire v. Canning, 2011 WL 90136 (S.D. Cal. Jan. 11, 2011).** The plaintiff filed a copyright infringement action against the defendant, a Canadian resident who uploaded, and then failed to remove, a video on YouTube. YouTube removed the video in response to a take-down notice from the plaintiff under the Digital Millennium Copyright Act, but reinstated it after a counter-notice from the defendant. Ruling on a motion to dismiss, the district court held, among other things, that the defendant consented to the jurisdiction of the court when she filed the counter-notice and invoked the benefits of the DMCA.

**Standard Chartered Bank Int'l (Americas) Ltd. v. Calvo, 2010 WL 2490995 (S.D.N.Y. June 16, 2010).** The plaintiffs applied for permission to file "a Complaint, the attached exhibits and all party filings" under seal in this action to enjoin an ongoing arbitration proceeding. The plaintiffs argued for sealing based on a confidentiality agreement stipulating that all arbitration materials would be kept private, and because information disclosed in a public filing would undermine a stay of discovery currently in place in a related securities litigation action. The district court denied the application and held: (1) the application was not based on concerns for "judicial efficiency" or "the privacy interests of innocent third parties," but to avoid scrutiny of issues of significant public concern that should not be kept secret; (2) the fact that the confidentiality agreement originated only several days before this application, even though the arbitration proceedings were filed nine months earlier, indicated that the plaintiff's concerns for privacy were not "in aid of arbitration, but an attempt to derail [it]"; and (3) because the application was ex parte, the defendants did not have an opportunity to be heard.

Copyright © 2011 The Sedona Conference®

***In re* Sept. 11 Litig. World Trade Ctr. Props, LLC. v. United Airlines, Inc., 733 F. Supp. 2d 526 (S.D.N.Y. 2010).** The New York Times (Times) intervened and moved to unseal a motion to approve a settlement relating to the September 11, 2001, terrorist attacks. The Times argued that the sealed filings are "judicial documents" subject to a strong presumption of public access under the First Amendment and the common law. The defendants argued that having relied upon the Sealing Order in order not "to chill" future settlements and to avoid any suggestion of fault for the September 11 attacks, the Times' motion should be granted only if the Sealing Order was inappropriate or there is an "extraordinary circumstance or compelling need justifying disclosure." The district court granted the Times' motion in part and denied it in part. The court, in vacating the part of the Order sealing information about the amount of the settlement and the allocation among the insurers, concluded that because this information bore directly upon the court's decision to approve the settlement, a strong presumption of public access applied and the reasons offered by the defendants for maintaining the seal were insufficient to outweigh the presumption. However, the court left in place the seal on the amounts to be paid to each plaintiff, concluding that the plaintiffs' privacy interests outweighed the presumption of access, and the court declined to unseal the confidential documents relating to damages recovery, negotiation, and mediation because these were "preliminary materials" with no bearing on the court's decision with respect to approval of the settlement and were not the kind of documents to which a presumption of access applies under the common law or the First Amendment.

**U.S. v. Dobbs, 629 F.3d 1199 (10th Cir. 2011).** The defendant was convicted of the knowing receipt of two images of child pornography found on the hard drive of his computer, in the temporary Internet files folder, or "cache." The Court of Appeals reversed, holding that a cache can be populated with images "regardless of whether they are displayed on the computer's monitor" and that "a user does not necessarily have to see an image for it to be captured by the computer's automatic-caching function." Absent evidence that the defendant had accessed the cached images or that he was aware of his computer's caching function, there was insufficient evidence that he had "knowingly" received the images

**United States v. Koch, 625 F.3d 470 (8th Cir. 2010).** During a valid search of the defendant's apartment for evidence of illegal gambling activities, law enforcement seized a computer and flash drive. After the defendant pled guilty to a gambling offense, law enforcement prepared to dispose of the seized items. An agent called a prosecutor for advice and then secured a disposal order from a State judge. Agents then viewed the contents of the drive and discovered images of child pornography. They then stopped the inspection, secured a search warrant for the computer, and discovered more images, after which the defendant was charged with possession. The district court denied a motion to suppress and found the defendant guilty after a bench trial. The Court of Appeals affirmed. The court concluded that the agents had acted in objective good faith in opening the drive. The Court of Appeals also, among other things, rejected the defendant's argument that there was insufficient evidence of knowing possession: There was evidence that the defendant had manipulated the images rather than that the images had been stored automatically in a cache. The court also affirmed a special condition that restricted his computer use and Internet access, noting that the defendant was a sophisticated computer user.

Copyright © 2011 The Sedona Conference®

**United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010).** The defendant, a former Social Security Administration employee, accessed SSA databases for confidential information about women with whom he had relationships. He did so in violation of a SSA policy that prohibited obtaining information for nonbusiness reasons. The defendant was convicted of violating the Computer Fraud and Abuse Act. The Court of Appeals affirmed. The defendant had "exceeded" his authorized access. The Court of Appeals also rejected, among other things, the argument that the Act required proof that use of information be in furtherance of some crime.

**United States v. Wright, 625 F.3d 583 (9th Cir. 2010).** During an undercover search on a file-sharing program, an agent came across a user name in chat rooms. The agent downloaded a number of files, some of which contained child pornography. After a search warrant was executed at the defendant's apartment, he was convicted of transportation and possession of child pornography. The Court of Appeals, among other things, reversed the transportation conviction as there was no evidence that the files were transported "in interstate commerce" as the pornographic images in issue had not "travelled" outside one state.

**Western Watershed Project v. BLM, 2010 WL 3735710 (D. Idaho Sept. 13, 2010).** The plaintiffs in this FOIA action requested that the Bureau of land Management (BLM) provide information concerning permits and permittees grazing livestock on public lands. The BLM provided the information requested for permittees formally organized and operating as businesses but withheld certain information on others (individuals, and family-owned and closely held entities) on the ground that such information was exempt from disclosure under Exemption 6. On cross-motions for summary judgment, the district court found that release of the information could result in the disclosure of individual home addresses and might lead to inferences concerning an individual's personal finances, information that qualified for nondisclosure under the "similar files" requirement of Exemption 6. However, in granting the plaintiffs' motion, the district court found that the public interest in the scope of the BLM's grazing and rangeland program was substantial and outweighed the permittees' privacy interests which did not rise to "a clearly unwarranted invasion of personal privacy" as required by Exemption 6.

**Wyeth v. Orgenus Pharma Inc., 2010 WL 4117157 (D.N.J. Oct. 19, 2010).** The defendant sought to compel the plaintiff to produce certain license and settlement agreements reached in prior litigation. The plaintiff objected, arguing relevancy and that third parties had a "confidentiality interest" in the documents. The district court held that the requested licenses and agreements were discoverable as these might lead to admissible evidence relating to (1) the plaintiff's claim for injunctive relief; (2) the defendants' invalidity defenses; (3) the issue of damages if defendants did an "at risk" launch of its product; and (4) a possible patent misuse defense and questions of "invalidity and obviousness." The district court concluded that other courts have "routinely recognized" that such license and settlement agreements are discoverable and that the plaintiff's concerns regarding third-party confidentiality interests did not outweigh the grounds to compel production.

Copyright © 2011 The Sedona Conference®

## STATE COURT DECISIONS

**Doe v. Corp. of the Presiding Bishop of the Church of Jesus Christ of Latter-Day Saints, No. 0710-11294 (Ore. Cir. Ct. June 18, 2010).** In this action involving allegations of child sexual abuse, the trial court ruled on a series of motions in connection with public access to certain files. The defendants asserted that the resolution of the issue was controlled by the First Amendment. The trial court disagreed, concluding that the Oregon Constitution, which "gives rights and protections for the public beyond the minimum standards" found in the United States Constitution governed the Oregon courts, and that the "open courts" provision of Article I, Section 10 of the Oregon Constitution mandates that justice be administered openly and without secrecy. The court found the defendants' assertion that public access to the information would taint the jury pool to be mere speculation. The court granted the motions but permitted release of the files with the names of the alleged victims and those who reported the alleged abuse redacted. Because the court considered the issue one of "first impression" it stayed its order to allow the defendants time for appellate review.

**Kieffer v. High Point Regional H.S., 2010 WL 5289002 (N.J. App. Div. Dec. 28, 2010).** This is an appeal from an order denying access to a public employee's letter of resignation as a baseball coach. The employee had been investigated in response to parental complaints and admonished for his behavior. He then resigned. The trial court, after a *in camera* review, found that the letter contained personal information exempt from disclosure under New Jersey statutory or common law. The Appellate Division affirmed: "The resignation letter explains the coach's personal reasons for resigning and contains confidential information. Stated plainly, it is none of the public's business."

**Mosallem v. Berenson, 76 A.D.3d 345 (N.Y. Sup. Ct. 2010).** In this action involving allegations of corporate corruption, the intervenor (a journalist) appealed from an order of the county court granting the defendants' motion to seal documents submitted. The Court of Appeals held that the defendants failed to establish good cause for sealing the documents. The Court of Appeals concluded that although the public's right to access is "not absolute," under New York law and the common law, there is a firmly grounded presumption of public access to judicial proceedings and court records to help assure that such actions are "conducted efficiently, honestly and fairly." The Court of Appeals held that there was no evidence in the record to justify restricting the public's access, and that the potential for embarrassment, harm to the defendants' business reputations, a general desire for privacy, or the possibility that the plaintiff obtained the documents by wrongful means did not constitute good cause. The Court of Appeals also rejected the lower court's finding that release of the documents would compromise federal grand jury secrecy because there had been no showing that the documents had been submitted to the grand jury or used in its deliberations.

Copyright © 2011 The Sedona Conference®

**O'Neill v. City of Shoreline, 240 P.3d 1149 (Wash. Sup. Ct. 2010).** In this Washington Public Records Act (PRA) action, the plaintiff, in responding to an allegation that she had sent an email claiming improper conduct by the City Council, asked for the email and all related information, and then "explicitly requested" all metadata relating to the email. The City sent the original email but not the associated metadata which was believed to have been "inadvertently destroyed." The trial court dismissed the complaint. The plaintiff appealed. The Washington Court of Appeals held that the metadata is a public record that must be disclosed under the PRA (which requires public access to all public records unless the record falls within specific exemptions), and that a public record request could be decided on the basis of affidavits alone, and remanded to permit the City to search for the metadata and to determine if the City had violated the PRA. The Court of Appeals also awarded attorney fees to the plaintiff. The Supreme Court affirmed except as to the award of attorney fees holding that none could be awarded unless the trial court found that the City had violated the PRA.

**People v. Diaz, 244 P.3d 501 (Cal. Sup. Ct. 2011).** The defendant challenged the fruits of the search of his cell phone. The defendant had been arrested after a controlled drug purchase and the phone seized incident to the arrest. Shortly after the arrest, the contents of the phone were searched and an incriminating message found. The defendant confessed after being confronted with the message. He moved to suppress, arguing that the warrantless search of the phone violated the Fourth Amendment. The motion was denied and the defendant pled guilty. The Court of Appeal affirmed. The California Supreme Court granted the defendant's petition for review. On the merits, and following "binding precedent" of the United States Supreme Court, the court held that the defendant's phone was "personal property" (not a "container") and that the warrantless search was valid, regardless of a delay in time. The majority rejected, over a vigorous dissent, the argument that the storage capacity of the phone was relevant and instead opted for a "bright-line" test.

**Pilchesky v. Gatelli, 2011 WL 17520 (Pa. Sup. Ct. Jan. 5, 2011).** The plaintiff appealed from an order in this defamation suit compelling disclosure of the identity of six anonymous individuals who the defendant claimed "pseudonymously" made defamatory statements about her on an internet message board maintained by the plaintiff. On cross-appeal, the defendant sought the identity of eight additional anonymous posters. The Supreme Court addressed the issue of whether ordering disclosure of the identity of the six anonymous posters violated their First Amendment rights. The Court held that collateral review was available on this and vacated and remanded on the merits. The Court held that trial court had realized the need to balance the competitive interests of the parties, but had failed (1) to require evidence sufficient to establish a prima facie case of defamation that would survive a motion for summary judgment; (2) to require an affidavit containing the assertion that the requested information related directly to the defendant's claim and was "fundamentally necessary" to secure relief, and (3) to conduct an explicit balancing of the posters' First Amendment rights against the strength of the defendant's prima facie case. The Pennsylvania Supreme Court further held that the defendant would be permitted to file an amended petition.

**Quinlan v. Curtiss-Wright Corp., 204 N.J. 239 (2010).** The plaintiff prevailed at a jury trial on her claims of discrimination and retaliation and the Appellate Court reversed. In reinstating the judgment, the New Jersey Supreme Court adopted a "totality of the circumstances approach" for determining the circumstances under which an employee "is privileged to take or to use"

Copyright © 2011 The Sedona Conference®

confidential documents of the employer. The Court established a multifactor test to balance the legitimate rights of an employer to conduct its business, including safeguarding its confidential documents, and the rights of an employee to be free from discrimination or retaliation. The Court held that the following factors must be evaluated: (1) how the employee gained possession or access to the documents; (2) what actions the employee took with respect to the documents; (3) the type and content of the documents to determine the degree of the employer's interest in keeping it confidential; (4) whether the employer had a clear policy on privacy or confidentiality that was violated by the employee's disclosure; 5) the relevance of the document in the particular circumstances balanced against the extent to which use or disclosure was "unduly disruptive to the employer's ordinary business"; (6) the "strength" of the employee's motivation for copying the document including whether, if not copied, the document might have been destroyed or discarded in the ordinary course of business; and (7) the broad remedial purposes served by the laws against discrimination and the effects of permitting or prohibiting use of the documents on the legitimate rights of both employers and employees.

**Republican Party v. New Mexico Taxation and Revenue Dep't, 242 P.3d 444 (N.M. Ct. App. 2010).** The plaintiffs in this Inspection of Public Records Act (IPRA) action appealed from an order of the district court granting summary judgment in favor of the defendants. The plaintiffs sought to discover personal driver's information to determine if "undocumented aliens were voting in federal, State, and local elections," and requested the information based on Section 14-2-5 of the IPRA which gives the "right to inspect any public records of [the] State except as otherwise provided by law." Although the defendants provided the records, much of the information was redacted in order to comply with State and federal laws limiting disclosure, executive privilege, or attorney-client privilege. In affirming the ruling of the district court, the Court of Appeals held (1) the redacted information met the definition of personal information protected from disclosure under the federal and State laws; (2) the IPRA specifically prohibited disclosure of documents subject to attorney-client privilege; and (3) while executive privilege is not absolute, the defendants met the burden of demonstrating that the public interest in preserving confidentiality of the documents outweighed the plaintiffs' interest in disclosure. The Court of Appeals also rejected the plaintiffs' argument that they were entitled to the information for "research activities."

**Reno Newspapers Inc. v. Haley, 234 P.3d 922 (Nev. 2010).** In this Nevada Public Records Act (the Act) action, the plaintiff appealed from an order which denied its petition for a writ of mandamus, on the ground that since an application for a concealed firearms permit is confidential under Nevada law, the requested records—pertaining to post-permit investigations, suspensions or revocations are also confidential because these would "necessarily contain information from the application." The Supreme Court reversed, noting that the Act considered all records to be public documents unless explicitly made confidential by statute or by balancing privacy and law enforcement interests against the public's right of access, and remanded for a determination of whether the post-permit records contained information that was made "explicitly" confidential under the statute. In doing so, the Supreme Court concluded that although the statute was clear and unambiguous in declaring that an application for a concealed firearms permit is confidential, the grant of confidentiality applies only to applications and permit investigations; it cannot be extended to cover post-permit information in light of (1) the consistent distinction made in the statute between an applicant and a permittee; (2) the legislature having made no "explicit grant" of confidentiality to a premittee; (3) the narrow construction of

Copyright © 2011 The Sedona Conference®

confidentiality required by the Act; and (4) the defendants' failure to meet the burden of proof required to demonstrate that private or law enforcement policy justifications for nondisclosure outweigh the public's right to access. The Supreme Court further concluded that if examination of the requested records revealed information "expressly declared confidential" by the statute, that information should be redacted and the remaining document made available to the plaintiff.

**Schill v. Wisconsin Rapids Sch. Dist., 786 N.W.2d 177 (Wis. 2010).** In this Wisconsin Public Records Law (PRL) action, the defendant appealed from a ruling by the trial court that ordered the release of all personal emails of the plaintiffs (public employees), to a third-party intervenor. The PRL gives the public access to records of "the affairs of government," "the official acts of officers and employees" and "the conduct of governmental business." In reversing and remanding to enjoin the defendant from releasing the plaintiff's personal emails, the Court held that to be a "record" under the PRL, the content of the document must be connected to a government function, and since the content of the e-mails "relate[d] exclusively to personal matters" these were not "records" and not subject to release, even though the emails were created and stored on government-owned computers.

**State v. Barger, 2011 WL 31786 (Ore. Sup. Ct. Jan. 6, 2011).** Interpreting State law, the Oregon Supreme Court addressed whether a person could be found guilty of 'possess[ing] or control[ling]' digital images of sexually explicit conduct involving a child …, based on evidence showing only that the person searched for and found such images through the Internet" on his … computer." An officer had looked at the defendant's computer with his wife's consent and seen suspicious addresses on the computer's "web-address history." The computer was thereafter seized (again, with the wife's consent) and the hard drive imaged. After the drive was examined, the defendant was charged based on eight images found in the "temporary internet file cache." After a jury conviction, the defendant appealed, arguing that that there was insufficient evidence of possession or control. The Court of Appeals affirmed. The Oregon Supreme Court reversed, holding that "the acts here in issue—navigating to a website and bringing the images that the site contains to a computer screen—are not acts that the legislature intended to criminalize." The court noted that the defendant could have been charged under Oregon law with *viewing* child pornography if that act had been accompanied by some payment.

**State v. McCraney, 2010 WL 5140789 (Ohio Ct. App. Dec. 15, 2010).** This is an appeal from the conviction of two defendant for criminal gang activity and other crimes. The Court of Appeals held, among other things, that evidence of photos posted on the defendants' MySpace pages (which showed them in gang-related conduct and attire) was sufficient to support the convictions.

**Stephens Media, LLC v. Eighth Judicial Dist. Court, 221 P.3d 1240 (Nev. 2009).** The plaintiffs sought a writ of mandamus challenging a ruling of the district court that denied the plaintiffs' application to intervene in a criminal action to obtain access to juror questionnaires. In reversing and directing the district court to release the blank and completed juror questionnaires, the Nevada Supreme Court concluded (1) the press and the public have a right to seek limited intervention in a criminal action to access court documents, based on the long standing presumption of open trials, including open jury selection, and the critical role such openness played in promoting public scrutiny of the judicial process, fairness of criminal proceedings, and public confidence in the criminal justice system; (2) the First Amendment right of access extends

Copyright © 2011 The Sedona Conference®

to juror questionnaires prepared in anticipation of the jury selection process; (3) a court may limit access to juror questionnaires with "specific findings" that such disclosure would deprive the accused of a fair trial and that no "alternatives to total suppression" exist; (4) release of a redacted version of the juror questionnaires after the trial ended was insufficient to meet the above requirements; and (5) the district court's concerns for juror candor and privacy which resulted in a "blanket promise" to keep the questionnaires confidential did not outweigh the press and the public's First Amendment right of access.

**SWB Yankees, LLC v. Wintermantel, 999 A.2d 672 (Pa. Commw. Ct. 2010).** In this Pennsylvania Right To Know Law (RTKL) action, the plaintiff (Yankees) appealed from an order of the trial court that denied and dismissed the plaintiff's petition for review and ordered the plaintiff to produce the requested information, *i.e.,* names and bids submitted to the Yankees for a concessionaire contract. The RTKL provides that a public record, legislative record, or financial record is open for public inspection and copying unless otherwise provided by law. In affirming the decision of the trial court, the Commonwealth Court held that the term "governmental function" in section 506(d)(1) covers operations of "a for-profit sports and entertainment venture" contracted to a third party by a local government agency, and that the requested records were public records because the plaintiff, in operating a public place for the benefit of the Commonwealth that created revenue for the Commonwealth, was performing a governmental function, and the records related to the amount of revenue generated.

**Too Much Media, LLC v. Hale, 993 A.2d 845 (N.J. App. Div. 2010).** The defendant appealed from a ruling in this defamation suit which denied her application for a protective order barring disclosure of the sources of her information, on the ground that she was not entitled to the protection of the New Jersey Shield Law. In affirming the ruling, the Appellate Division concluded that the New Jersey Shield Law focuses on the news process as opposed to the medium by which the news is disseminated, and that the key to garnering the protection of the Shield Law is not having a website or proclaiming oneself a reporter, but involvement in activities traditionally associated with the gathering and dissemination of news. The Appellate Division held that the defendant "exhibited none of the recognized qualities or characteristics traditionally associated with the news process, nor ha[d] she demonstrated an established connection or affiliation with any news entity" (emphasis in original). The Appellate Division also held that the Shield Law was not applicable where, as here, the defendant never identified herself to the sources as a reporter or journalist, where there was no evidence of any agreement of confidentiality with the sources, and where there was no evidence that the defendant's outlet qualified as a "news media." The Appellate Division rejected the defendant's argument that the First Amendment provided an independent basis for protecting the identity of her sources, holding that there is no distinction between the protection afforded under the New Jersey Shield Law and the First Amendment.

**Yakima County v. Yakima Herald-Republic, 2011 WL 113764 (Wash. Sup. Ct. Jan. 13, 2011).** Attorneys were assigned to represent two indigent murder defendants in separate trials and the attorneys made various *ex parte* applications for funding and reimbursement of, among other things, experts. All of the financial documents were placed under seal. The appellant newspaper moved to intervene to challenge the sealing. After the motions were denied, the Washington Supreme Court held (1) The documents in issue were "judicial" is nature and not subject to the Washington Public Records Act; (2) any documents transferred to a county were

Copyright © 2011 The Sedona Conference®

subject to the PRA absent a protective order; (3) trial court had jurisdiction over motions to intervene in criminal actions even if appeal is pending as resolution of motion will not impact any appellate ruling. Among other things, the court recognized that there was no historical access to the *ex parte* proceedings that had been conducted below and remanded for *in camera* review.

Copyright © 2011 The Sedona Conference®