



Monday, October 20
11:00 am-12:30 pm

108 Ethics Issues Surrounding Electronic Discovery

Jack Halprin
Director, eDiscovery
Zantaz

Jayne Rothman
Corporate Counsel
EPIQ Systems, Inc.

Eric J. Schwarz
Discovery Services Practice Leader
Ernst & Young LLP

Brett Tarr
Legal Counsel
eMag Solutions LLC

Faculty Biographies

Jack Halprin

Jack Halprin is director, eDiscovery, for Autonomy, Inc. in San Francisco. Mr. Halprin manages the product line strategy for Autonomy's legal hold and early case assessment solutions, speaking frequently on enterprise legal risk management and eDiscovery at industry events and seminars. Mr. Halprin is also actively involved in the Electronic Discovery Reference Model (EDRM) forum, currently leading the EDRM Metrics 3 working group.

Prior to joining Autonomy, Mr. Halprin was with Guidance Software as senior product marketing manager/product manager for eDiscovery, where he developed business partnerships, drove product development, conducted research, and created integrated marketing efforts for EnCase eDiscovery. Mr. Halprin also served as corporate electronic discovery specialist at LexisNexis Applied Discovery, increasing company knowledge of eDiscovery-related topics and delivering Continuing Legal Education sessions for corporate legal departments. Prior to working in the eDiscovery field, Mr. Halprin worked for BAR/BRI Bar Review, where he created and launched a patent bar review program and delivered lectures for both the patent bar exam and state bar exams. Mr. Halprin also served as a litigation associate at Santa Monica's Haight, Brown & Bonesteel.

Mr. Halprin received a BA from Yale University, and is a graduate of the University of California-Los Angeles School of Law.

Jayne Rothman

Jayne Rothman is corporate counsel to Epiq Systems, Inc. and its subsidiary companies in New York.

Prior to joining Epiq, Ms. Rothman worked at Dewey Ballantine LLP in Los Angeles, representing creditors in the WorldCom Chapter 11 case, five aircraft lessors and two real property lessors holding filed claims of nearly \$1 billion in the United Airlines Chapter 11 case. Ms. Rothman also represented ABC/ESPN in the restructuring of its contracts with Adelphia Communications and the resolution of existing contract issues and claims in the Adelphia Chapter 11 case, among others. Prior to that, Ms. Rothman practiced corporate M&A and business financial and restructuring law at Weil Gotshal & Manges LLP in New York, representing corporate clients including Enron Corp., Hughes Electronics Corp., Old Mutual Pic., Six Flags, Inc., Urban Box Office.com, and John Wiley & Sons, Inc.

Ms. Rothman received a BA with honors from the University of New Hampshire and is a graduate of New York Law School.

Eric J. Schwarz

Eric J. Schwarz is the discovery services practice leader for Ernst & Young in Dallas. As a thought leader and testifying expert in the fields of electronic discovery and computer forensics, Mr. Schwarz has worked on matters such as insider trading investigations, foreign regulatory agency investigations, intellectual property disputes, Securities and Exchange Commission investigations, parallel proceedings and multi-state class action lawsuits.

Mr. Schwarz is also a participant of the Sedona Conference working group on best practices for electronic document retention and production, and serves as one of the co-chairs of Sedona's litigation hold special project team.

Mr. Schwarz received a BA from the University of Western Ontario and a MBA from Boston University.

Brett Tarr

Brett Tarr serves as general counsel for eMag Solutions, based in Atlanta.

Prior to joining eMag, Mr. Tarr worked as a practicing attorney at King & Spalding LLP, and has held chief operating officer, legal counsel, and senior marketing executive positions for several corporations over the past 10 years.

Mr. Tarr has published articles on multiple topics involving electronic discovery, legal preparedness, and data security, among others.

Mr. Tarr graduated Phi Beta Kappa from the University of California at Los Angeles, and also holds a MBA in Marketing and Management from Georgia State University. Mr. Tarr earned his JD from Duke University School of Law.



Agenda

- **How to best preserve attorney client privilege**
- **What are the ethical implications of outsourcing**
- **Our own technological competency (or lack thereof)**
- **Ensuring confidentiality of client information**
- **Requirements regarding keeping paper records copies**
- **Storing client information**
- **Inadvertent disclosure of electronically stored information**
- **Implications of accessing metadata and spyware**
- **Rules regarding internet discussion groups**
- **Email interception**
- **Preservation duties**
- **Spoliation sanctions**
- **Risk management**
- **Best practices for managing discovery and litigation**



Ethics Topics in E-Discovery

- **Impact of new Federal Rules on ethical obligations**
- **Duties when faced with inadvertent disclosure of adversaries' documents**
- **Relevant ethical rules**
- **Review of metadata implications**
- **Special considerations for corporate counsel**
- **Scope of the safe harbor rule 37(f)**
- **Ethical issues surrounding the preservation of electronic documents**
- **Questions surrounding "meet and confer" obligations, including repercussions of saying nothing and providing nothing**
- **Attempts to shield production of electronic documents**
- **Inadvertent production of privileged documents**
- **Disclosure of search criteria**
- **Disclosure of metadata**
- **Interception of email**
- **Standards for use of technology by attorneys**



Ensuring Confidentiality

Florida Ethics Opinion 06-2 states that a lawyer who is sending an electronic document should take care to ensure the confidentiality of all information contained in the document, including metadata

Rule 1.6 and DR 4-101 are the principal provisions requiring lawyers to protect client information. The ways in which a lawyer can violate her duties of confidentiality to her client through the misuse of technology are virtually endless.

Misdirected Facsimiles or E-mails

It is possible to send a fax or an E-mail to the wrong person, thereby disclosing client confidences to someone who should not have them. Speed dialing and the ability to send documents to multiple locations increase the danger. No case law or ethics opinion holding that misdirecting a fax or E-mail violates the ethics rules on confidentiality; however, lawyer carelessness in this regard could lead to such a finding.

A lawyer receiving an electronic document should not try to obtain information from metadata that the lawyer knows or should know is not intended for the receiving lawyer. A lawyer who inadvertently receives information via metadata in an electronic document should notify the sender of the information's receipt



Requirements about keeping paper records copies

- **06/03/06: Virginia lawyers may maintain client files exclusively in electronic format without any paper copies as long as the client's interests are not prejudiced. Lawyers may also destroy paper copies as long as the client consents. The only exceptions are items that have independent legal significance such as testamentary documents and marriage certificates.**
Virginia St. Bar. Standing Comm. on Legal Ethics, Op. 1818



Storing Client Records

- 06/03/06: Law firms may store electronic client records on third party remote servers as long as the firm selects the company with care and the company agrees to keep the information confidential.
Nev. St. Bar Standing Comm. on Ethics and Professional Resp. Formal Op. 33
- On February 9, 2006, the Nevada Bar Association issued an opinion saying it was proper to outsource electronic storage of client files to third parties, so long as the lawyer acts reasonably to safeguard the files
- The Arizona State Bar Association in July 2005 issued Opinion 05-04 which holds that it is permissible for lawyers to store client data on a computer which is connected to the Internet, but only if the lawyer takes "reasonable steps" to assure that the confidentiality over such information is not lost through inadvertence or theft



Rules Regarding Internet Discussion Groups

- Lawyers who participate in Internet discussion groups should avoid including any confidential information that could be associated with a particular case or controversy. Postings that give identifying details about cases can result in problems such as waiver of work product protection or inadvertent communications with judges involved on a case
- On August 19, 2005, the Professional Responsibility and Ethics Committee for the Los Angeles Bar Association issued Formal Op. 514, holding that attorneys should avoid including any confidential or private information in a Listserv or other Internet posting that could be identified to a particular case or controversy.



Spyware

- A lawyer was suspended in late 2005 by the Minnesota Supreme Court for installing spyware on a computer.



Metadata

- January 6, the Florida Bar took the position that mining metadata is unethical
- The New York Bar Association acknowledges in an ethics opinion that under some circumstances there may be a duty to avoid disclosure of metadata and similar hidden information



Metadata Removal

- The ABA suggests that lawyers filter out, or "scrub", metadata in documents before sending them
- This can invite sanctions if the removal of metadata was not previously negotiated
- The first step towards limiting opposing counsel's use of your client's metadata is to negotiate an agreement with opposing parties about the forms of production and inclusion of metadata
- Attorneys should also attempt to negotiate confidentiality agreements or protective orders that cover metadata, or object to the production of metadata before the judge.



Email Interception

- On August 11, 2005, the First Circuit issued its en banc decision in *U.S. v. Councilman*, 2005 WL 1907528 (1st Cir. Aug. 11, 2005), where it held that interception of e-mail while on its way to the recipient violated the Electronic Communications Privacy Act. This case lends strength to the position of those who believe that attorneys may use e-mail without encryption.
- 11/05/04: The First Circuit vacates its prior opinion in *U.S. v. Councilman* (1st Cir. 2004), which held that the ECPA does not prevent interception of e-mail as it is stored in a router. The First Circuit is taking the case for *en banc* rehearing. The outcome could be important to the question of whether lawyers can send plaintext (unencrypted) e-mail.



Preservation Duties, Spoliation Sanctions, and Risk Management

- Management strategies for avoiding spoliation of evidence
- Reducing the risk of sanctions
- Proportionality matrix - measuring good faith, due diligence, risk of spoliation, and adverse consequences
- Saving what you need to save and being able to produce it



Technology and Competence

- The first rule in legal ethics is that a lawyer must be competent. Failure of a lawyer to use technology properly can lead to client harm and thus the claim that the lawyer has acted incompetently.
 1. *Backup*
The failure of a lawyer to back up her computer system could result in the loss of crucial client data.
 2. *Viruses*
Failure of a lawyer to use standard antivirus software can cause the loss of crucial client data.
 3. *Electronic Filing*
Some tribunals and government agencies require electronic filing. Some prohibit electronic filing. Thus, failure to know the difference can cause harm to a client.



Hardware Abuses

- Lawyers increasingly send documents as E-mail attachments. However, some still use floppy disks. Failure to use new, or "fresh," floppies could result in a breach of client confidentiality. For example, it may be possible for the recipient to detect earlier drafts of the subject document. Or the floppy could contain confidential information of other clients.
- Steps should be taken to ensure that hardware that is scrapped, traded in, or sold does not contain client information. Likewise, hardware that is rented or leased should be checked for client information before being returned to its owner.



Inadvertent Disclosure of Electronically Stored Information

- Ethical duties if opponent inadvertently produces
- Inadvertent production as possible waiver under applicable law of jurisdiction
- *Rico v. Mitsubishi Motors* (2007), Cal.4th (Filed 12/13/07)
 - "When a lawyer who receives materials that obviously appear to be subject to an attorney-client privilege or otherwise clearly appear to be confidential and privileged ... where it is reasonably apparent that the materials were ... made available through inadvertence, the lawyer receiving such materials should refrain from examining the materials any more than is essential to ascertain if the materials are privileged, and shall immediately notify the sender that he or she possesses material that appears to be privileged.



Best Practices for Managing Discovery & Litigation

- Build an in-house team to formulate and enforce best practices for electronic discovery
- Understand what data your organization has and where/how it is stored via data mapping
- Develop effective retention policies to avoid over-producing ESI
- Identify your E Discovery allies at outside law firms
- Leverage technology to realize true cost savings by internalization and matter synergy
- Implement strategic technical and policy initiatives to fulfill discovery obligations efficiently
- Recognize the benefits of search and retrieval technology
- Select vendors and maintain vendor relationships using the RFP Process