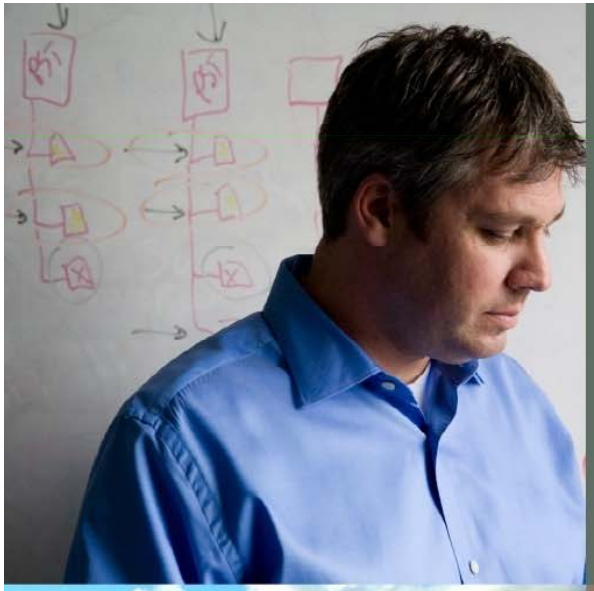
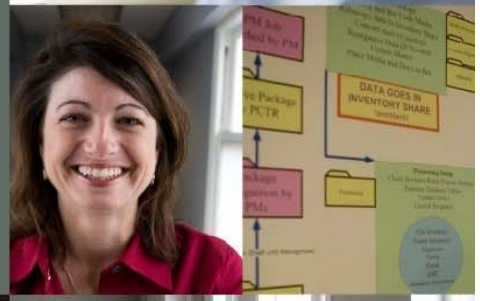


The Sedona Conference® Update: White Collar Crimes & e-Discovery Implications



October 14, 2008

About Fios

For over a decade, Fios has helped corporations and their outside counsel reduce risk, control costs and gain management control over the entire spectrum of e-discovery. We are dedicated exclusively to delivering comprehensive services and expert guidance that transform the burdensome nature of electronic discovery into a streamlined, legally defensible business process. Our proven services and methodologies are based on an integrated, in-depth knowledge of technology, legal and human resource requirements to meet the ever-changing demands of complex e-discovery.

About The Sedona Conference

The Sedona Conference® is a nonprofit, 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. Through a combination of Conferences, Working Groups, and the "magic" of dialogue, The Sedona Conference® seeks to move the law forward in a reasoned and just way. The Sedona Conference® succeeds through the generous contributions of time by its faculties and Working Group members, and is able to fund its operations primarily through the financial support of its members, conference registrants, and sponsorships.

Upcoming Fios' Webcasts

Webcast	Date	Speaker(s)
e-Discovery for Financial Services/Subprime Litigation Webcast Series	10/01/08 to 11/20/08	• 8-part webcast series featuring industry experts and attorneys addressing e-discovery in the wake of the financial crisis
Discovery Readiness: Know Where You Are, Where You're Going and How to Get There	10/28/08	• Peter McLaughlin, Director, Fios Consulting • Cynthia Bateman, Esq., Senior Manager, Fios Consulting
The Legal Hold Process - Automated Legal Hold Management	11/05/08	• Brad Harris, Director, Fios Consulting • Mandana Salehi, Senior Director of Business Development, Exterro

Guest Faculty

Daniel Gelb, Esq.
Associate, Gelb & Gelb LLP

- Represents clients in federal and state court litigation, arbitration and regulatory proceedings
- Concentrates in the areas of business, securities, non-competition agreements, corporate raiding and trade secrets, accountants' liability and criminal law.
- Prior to joining Gelb & Gelb LLP, Mr. Gelb was an Assistant District Attorney for over two years with the Norfolk County District Attorney's Office where he prosecuted various criminal matters
- Member of:
  - Advisory Board for the Bureau of National Affairs, Inc.'s *White Collar Crime Report*
  - The Sedona Conference Working Group on Electronic Document Retention and Production
  - The National Association of Criminal Defense Lawyers' Electronic Discovery Task Force
  - The Massachusetts Bar Association's Civil Litigation Section Council where he chairs its Electronic Discovery Practice Group.
  - Massachusetts Academy of Trial Attorneys
  - Massachusetts Association of Criminal Defense Lawyers
  - Criminal Law Section of the Boston Bar Association
  - American Bar Association's White Collar Crime Young Lawyers Steering Committee
- Graduated from Tufts University (B.A. in English 1999), Boston College Law School (J.D. 2003) and Boston College Carroll Graduate School of Management (M.B.A. 2003).

Guest Faculty

Cecil A. Lynn III, Esq.
Of Counsel, Riley Carlock & Applewhite

- Recognized thought leader in the area of electronic discovery and an accomplished trial lawyer
- Enjoys a very diverse practice area, which includes representing clients on issues related to intellectual property, employment, sports, entertainment, and white-collar crime
- Speaks and publishes on a wide variety of e-discovery topics including, document review, document retention, data accessibility and international e-discovery
- Active member of the Sedona Conference® and serves as an instructor for the National Institute for Trial Advocacy (NITA)
- Prior to joining RCA, he was the Director of Industry Relations at one of the largest e-discovery companies in the industry
- He previously served as a trial attorney for the Civil Rights Division, Criminal Section of the U.S. Department of Justice and also served as a special prosecutor for the National Church Arson Task Force
- Former adjunct professor at Loyola Law School in Los Angeles, California and he is currently an instructor at Cal State University, Fullerton
  Holds a B.A., with University Honors, from New Mexico State University and a J.D. from the University of California, Hastings College of the Law

Moderator

Mary Mack, Esq.
Corporate Technology Counsel, Fios, Inc.

Mary Mack has more than 10 years experience handling electronic material for legal purposes and 20 years experience delivering enterprise-wide software projects with IT departments in publicly-held companies. A member of the Illinois Bar, ACC and the ABA's Section on Litigation, Mack received her J.D. from Northwestern University School of Law (1982) and a B.A. from LeMoyne College in Syracuse, NY. Mack is the author of the book entitled, *A Process of Illumination: The Practical Guide to Electronic Discovery*, the author of the *Sound Evidence* blog hosted on DiscoveryResources.org, and the co-editor and contributor to *e-Discovery for Corporate Counsel* published by Thompson Reuters *West.*

E-Discovery In Criminal Litigation

- Characteristics pertaining to ESI and e-discovery (e.g., volume, volatility, metadata, etc.) influenced the development *The Sedona Principles* and the subsequent amendments to the Federal Rules of Civil Procedure.

- An increased danger of inadvertently producing privileged information pose challenges for as much for criminal lawyers as for civil litigators—but the challenges are different.

- *U.S. v. O'Keefe, 2008 WL 449729* (D.D.C., Feb 18, 2008) (addressing the impact of the evolution of e-discovery in civil litigation on criminal litigation matters)

Government's Legal Authority to Seek e-Discovery

- Law governing electronic evidence in criminal investigations has **two (2) primary sources**:

  (1) Fourth Amendment to the U.S. Constitution; and

  (2) Statutory privacy laws codified at 18 U.S.C. §§ 2510-22 (*The Wiretap Statute*); 18 U.S.C. §§ 2701-12 (*Electronic Communications Privacy Act*); and 18 U.S.C. §§ 3121-27 (*The Pen/Trap Statute*)

Subpoena Duces Tecum

- Fed. R. Crim. Proc. 17
  - Grand jury has considerable discretion to order a witness to produce books, papers, documents, data, or other items designated in a subpoena.
  - Unlike search warrants, there is no probable cause requirement inherent in the grand jury's issuance of a subpoena
- Administrative Subpoenas
  - Probable cause is not required to support an administrative subpoena.

Subpoena Duces Tecum

- Subpoena must be reasonable:
  1. Subpoena can seek only the production of things relevant to the investigation being pursued;
  2. The subpoena must specify the items to be produced with reasonable particularity;
  3. The subpoena may only request documents covering a reasonable period of time.

Subpoena

- The subpoena can seek only the production of things relevant to the investigation being pursued;
- The subpoena must specify the items to be produced with reasonable particularity; and
- The subpoena may only request documents covering a reasonable period of time.

Subpoenas

1. Preserve All Potentially Relevant Electronically Stored Information.
2. Ascertain Whether the Corporation, its Officers, or Employees are Targets of the Investigation.
3. Determine Whether Compliance With the Subpoena is Possible Given the Amount of Requested Material as Compared to the Allotted Time
4 Meet and Confer with Government Specifically Relating to Electronically Stored Information.
5. Resist Calls for the Production of the Virtual “File Cabinet” Where Targeted Search and Collection Efforts Work Better for the Corporation and the Government.
6. Take Adequate Steps to Ensure the Corporation Does Not Produce Privileged and Protected Materials.
7. Recognize that if the Cost of Subpoena Compliance is Oppressive, The Court May Order The Government to Copy and Review the Material in Lieu of Cost Shifting
8. Consider Using Neutral Third Party to Collect Data

Responding to Search Warrants v. Subpoenas

- Many of the considerations that go into responding to a subpoenas are relevant to issues related to complying with a warrant to search for electronic information.
- The major difference between Subpoenas and Search Warrants:
  - Timing
  - Element of surprise

Search Warrants

- A search warrant (1) must state with reasonable particularity what items are being targeted for search and seizure; or in the alternative, (2) what criminal activity is suspected of having been committed.

- *U.S. v. Comprehensive Drug Testing, Inc., 513 F.3d 1085* (9th Cir. 2008) (government's affidavits were premised on the advice of computer specialists who anticipated that certain intermingled evidence might be difficult to separate on-site).

Search Warrants

1. Follow Company's Internal Guidelines for Compliance with Search Warrant
2. Obtain a Copy of the Search Warrant and Read it Carefully
3. Contact Outside Counsel and Ask the Lead Agent to Wait for the Attorney's Arrival Before Commencing with the Search
4. Be Cooperative But Do Not Consent to the Search
5. Determine Whether the Agents Have a Search Protocol for Electronically Stored Information
6. Determine Whether Search Warrant and/or Protocol Adequately Protect Attorney-Client Privileged Documents or Other Protected Information.
7. Proactively Monitor Search and Double-Check the Agent's Receipt of Inventory
8. Enforce Legal Rights if Search is Invalid or Unlawful

Search Warrants

- Determine whether search warrant and/or protocol adequately protect attorney-client privileged documents or other protected information.

- Once the potentially privileged or protected information has been segregated, the government has several options to determine whether the data is in fact protected.

    1. Taint Teams

    2. Special Master

    3. In Camera Review

Federal Rule of Evidence 502

- *Take adequate steps to ensure the corporation does not produce privileged and protected materials.*
- Entity generally waives privilege by disclosing protected information “unless that disclosure is made to a federal, state, or local governmental agency during an investigation by that agency....”
- FRE 502 will likely *not protect* against collateral administrative and/or regulatory enforcement

Fifth Amendment

- Applies wherever and whenever an individual is compelled to testify
- Right against self-incrimination applies whether the witness is in Federal or state court (see *Malloy v. Hogan*, 378 U.S. 1 (1964)), and whether the proceeding itself is *criminal or civil* (see *McCarthy v. Arndstein*, 266 U.S. 34 (1924))
- A corporation has no Fifth Amendment privilege against self-incrimination or a right to privacy

Fifth Amendment:
Statements by individuals v. by corporation

- The information that government seeks to seize from the computer;
- The methods used to locate that information without generally reviewing all information on the computer, and manner of assistance provided to government;
- Whether agents intend to search the computer and make electronic copies of specific files or to duplicate entire storage devices for later off-site review.
- ***"Required Records Doctrine"*** (Fifth Amendment applicable to one's papers and effects, but it does not extend to corporate persons, therefore corporate records are subject to compelled production.).

Sixth Amendment

- Obstruction of Justice (18 U.S.C. §§ 1512(c), 1519) will destroy the attorney-client relationship
- *United States v. Stein*, 2007 U.S. Dist. LEXIS 52053 (S.D.N.Y. July 16, 2007)
  - The court's opinion described the impact of the government-coerced decision of KPMG not to pay legal fees upon the defendants.
  - Impacts included the ability of the defendants to engage in electronic discovery.
  - ESI needs should not compromise right to counsel.

Chain of Custody

- Who collected it? (i.e., devices, media, associated peripherals, etc.)
- How and where? (i.e., how was the evidence collected and where was it located)
- Who took possession of it? (i.e., individual in charge of seizing evidence)
- How was it stored and protected in storage? (i.e., evidence-custodian procedures)
- Who took it out of storage and why? (i.e., on-going documentation of individual's name and purpose for checking-out evidence)

(National Institute of Standards and Technology)

U.S. v. Graham, 2008 WL 2098044 (May 16, 2008)

- U.S. v. Graham, 2008 WL 2098044 (May 16, 2008), the Court shared responsibility for the "procedural predicament" of the case.
- Government cannot be permitted to remain inert in the face of large volumes of unsorted discovery materials. Nor can the government be permitted to refuse to share databases and search engines with defense counsel.
- Taxpayers should not be required to fund two separate means for managing and searching electronically recordable data-one for the government and one for the defense.
- E-discovery must be provided in virus-free, non-corrupt form.
- Court should establish deadlines for government production of discovery.
- Defense counsel bears some responsibility for not bringing problems encountered in the course of discovery to the attention of the Court in a prompt manner."

Suppression Issues

- Was the evidence obtained either pursuant to a **search warrant** or as a result of gaining consent?
- If it was seized **without a warrant or consent**, was the ESI seized pursuant to a well-founded **legal exception**?
- Can the evidence be considered **testimonial**?
- Was the **content** seized the subject of **statutory protection** (e.g., Pen/Trap, Wiretap, ECPA, HIPPA, Graham-Leach Bliley)?
- Was the ESI seized described in the affidavit to the search warrant and within its **scope**?
- Was the evidence obtained from a **third party** custodian or the defendant and how has it been used (e.g., Grand Jury)?
- Is the evidence **derived** from *Brady* material?
- **Chain of custody** and forensic and non-forensic **audit trail**?

Get an Expert Because the Government Has One

- Avoid internal investigation pitfalls
- Qualifying the Expert
  - Experience
  - Responsibilities
  - Technological Background
  - Law Enforcement Experience
  - Computer Search and Seizure Experience
  - Experience With Authoring Search Warrants
  - Number of Searches Conducted
  - Background in Forensics (e.g., certified)
  - Testimonial Experience

How Fios Can Help

Fios offers comprehensive consulting services to help corporations and outside counsel address e-discovery challenges related to internal and government investigations, including:

- e-Discovery Readiness and Planning
- Records Retention and Assessments
- Legal Hold Management/Workflow
- Technology Assessment and Consulting

For a complete overview of Fios' services, visit www.fiosinc.com

Questions

e-Discovery Resources

- The Sedona Conference
  - www.thesedonaconference.org
- Fios' Webcasts & Articles
  - www.fiosinc.com/resources
- Fios-Sponsored Resources
  - DiscoveryResources.org - www.discoveryresources.org
  - Sound Evidence Blog - Soundevidence.discoveryresources.org
- Contact Information:

Cecil A. Lynn, III, Esq.
Ryley Carlock & Applewhite , P.A.
(602) 440-4827
clynn@rcalaw.com

Daniel K. Gelb, Esq.
Gelb & Gelb LLP
(617) 345-0010
dgelb@gelbgelb.com

Mary Mack, Esq.
Fios, Inc.
503-265-0711
mmack@fiosinc.com