Tuesday, October 21
4:30 pm-6:00 pm

708 Hot Topics in E-Discovery: Are There Any Other Kinds?

Henry K. Hamilton
Director and Corporate Counsel
Starbucks Coffee Company

The Honorable Timothy Hillman
US Magistrate Judge
US District Court for the District of Massachusetts

Linda M. Kearney
Managing Associate General Counsel
Wellpoint, Inc.

Monica Palko
Associate Corporate Counsel
Bearing Point, Inc.

Michael J. Tuteur
Partner
Foley & Lardner LLP

Faculty Biographies

Henry K. Hamilton

Henry K. Hamilton is a director and corporate counsel for Starbucks Corporation in Seattle. Mr. Hamilton manages Starbucks' global litigation involving real estate and commercial disputes. In this role he founded and currently leads the electronic discovery team. This cross-functional team focuses on e-discovery issues, records security, and risk avoidance. In addition, Mr. Hamilton counsels his clients on environmental matters, construction issues, bankruptcy, and regulatory affairs.

Prior to joining Starbucks, Mr. Hamilton practiced law in Seattle for nearly twenty years. He is a former shareholder in the Seattle office of Stafford Frey Cooper and a former member of Grieff & Hamilton, PLLC. In addition, Mr. Hamilton also acted as deputy general counsel for Wizards of the Coast, where he managed its litigation. Prior to law school, Henry briefly worked as an engineer.

Mr. Hamilton is the current chair of the Washington State Bar Association corporate counsel section. He also previously served on the executive council of the American Bar Association Young Lawyers Division and on the governing committee of the American Bar Association forum on the construction industry.

The Honorable Timothy Hillman

Judge Timothy Hillman is a United States Magistrate Judge for the District of Massachusetts.

Prior to his appointment as a magistrate judge, Judge Hillman was a judge of the Massachusetts Superior Court from 1998-2006. Prior to that, he was an associate justice and presiding justice in the Gardner District Court and the presiding justice in the Worcester District Court. Judge Hillman was also in private practice for a number of years, and during that time he served in the Worcester County District Attorney's Office, and as town counsel and city solicitor for several Massachusetts communities.

Judge Hillman has taught law and psychiatry at the Massachusetts School of Law and trial advocacy at Clark University. In addition, Judge Hillman was the project executive for Massachusetts Trial Court's Information Technology Project and was responsible for the procurement and implementation of a statewide integrated case management and docketing system for all levels of the Massachusetts trial court system.

Judge Hillman received a BA from Coe College and is a graduate of Suffolk University Law School.

Linda M. Kearny

Linda M. Kearney is managing associate general counsel for WellPoint, Inc. in their Austin office. Ms. Kearney serves on WellPoint's litigation management team, where her primary responsibilities include managing litigation nationwide for WellPoint's UniCare/HealthLink subsidiaries. Ms. Kearny was also the team leader for the company's outside counsel convergence initiative.

Prior to joining WellPoint, Ms. Kearney was a partner at the law firm of Porter, Rogers, Dahlman & Gordon, P.C., in Corpus Christi, TX, where she primarily handled insurance and health law related litigation. Ms. Kearney also served as assistant attorney general in the Law Enforcement Defense Division of the Texas Attorney General's Office.

Ms. Kearney is the secretary of ACC's Litigation Committee. She has also served as an elected officer or appointed official for several other law related organizations, including serving as the district chairperson presiding over grievance hearings for attorneys in Texas who have been accused of professional misconduct. Ms. Kearney is board certified in Civil Trial Law by the Texas Board of Legal Specialization.

Ms. Kearney received a BA from The George Washington University and is a graduate of the University of Notre Dame Law School.

Monica J. Palko

Monica J. Palko is associate corporate counsel, litigation, for BearingPoint, Inc., one of the world's leading consulting firms, in Arlington, VA. BearingPoint provides strategic consulting, information technology solutions, and managed services to Global 2000 companies and government organizations worldwide. Ms. Palko handles a varied caseload, including litigation regarding commercial and government contracts, corporate governance, and compliance.

For several years prior to joining BearingPoint, Ms. Palko was a trial attorney in the commercial litigation branch of the Civil Division of the U.S. Department of Justice in Washington, DC, where she was responsible for defending trial and appellate-level commercial litigation pursued against the United States. Before joining the Department of Justice, Ms. Palko was an associate at Bracewell & Giuliani LLP (then Bracewell & Patterson LLP) where she handled general civil litigation.

Michael J. Tuteur

Michael J. Tuteur is a partner and co-chair of the litigation department in the Boston office of Foley & Lardner LLP. His practice specialties include complex civil litigation, False Claims Act defense, securities enforcement litigation, and white-collar criminal defense. Mr. Tuteur's recent cases include successfully defending an independent state authority in a $100 million False Claims Act appeal in the DC Circuit; obtaining a $200 million judgment in connection with the demutualization of a major life insurance

company; and winning summary judgment for a global advertising company against a "raiding" claim based in the Ukraine. Mr. Tuteur is also currently representing key individuals in DOJ and SEC investigations involving revenue recognition, hedge accounting for derivatives, and the offering of gifts and gratuities in the financial services business.

Prior to joining Foley & Lardner, Mr. Tuteur served as an assistant US attorney in the District of Massachusetts, where he worked in both the major crimes and organized crime strike force units.

Mr. Tuteur currently serves on the advisory committee on local rules for the US District Court for the District of Massachusetts, and as trial advisor in Harvard Law School's Trial Advocacy Workshop.

Mr. Tuteur received his AB, summa cum laude, from Harvard College and his JD, magna cum laude, from Harvard Law School.

Electronic Discovery Disasters

***Qualcomm, Inc. v. Broadcom, Corp.,* 2008 U.S. Dist. Lexis 911 (S.D. Calif. 2008)**

- Qualcomm failed to produce "tens of thousands of e-mails"
- Ordered to pay Broadcom's legal bills -- more than $8.5 million.
- Six of Qualcomm's outside attorneys, referred to the State Bar for discipline.

Electronic Discovery Disasters

***In re Intel Corp. Microprocessor Antitrust Litig.*, 2008 WL 2310288 (D. Del. 2008)**

- Intel's ESI preservation activities did not, *inter alia*, include suspension of the "auto delete" function of its email system - automatically deleted emails remaining in an employees mailbox after 35 days
- Intel relied upon individual custodians (i.e., employees) to identify, segregate and move relevant evidence to storage or their local computer before that data was destroyed by a network purge

Electronic Discovery Disasters

In re Intel Corp. Microprocessor Antitrust Litig.

- Intel claimed that its retention lapses were the result of human error and not the result of deliberate deletion
- Intel filed summaries based on its attorneys' interviews of more than 1000 employees concerning compliance with their evidence preservation obligations
- Court determined Intel waived attorney client privilege and ordering Intel to produce notes of its counsel's investigation interviews

Electronic Discovery Disasters

Keithley v. The Homestore.com

- After plaintiff filed motion for sanctions - CTO had "resurgence of memory" and found a backup of the source code
- Later that month, an engineer found more of the source code in question in a drawer in her cubicle. (Court deemed the drawer to be "readily accessible.")

Electronic Discovery Disasters

***Keithley v. The Homestore.com*, 03-4447. (N.D. Cal. August 12, 2008)**

- Litigation threatened in 2001
- Defendant's chief technology officer testified that database with the source code in question had been eliminated in 2001 during a transfer to a new system.
- CTO testified that a 2004 catastrophic computer failure wiped out the code.

Electronic Discovery Disasters

Keithley v. The Homestore.com

- Defendants ordered to pay more than $250,000 in monetary sanctions in addition to evidentiary sanctions
- Court noted that Defendants lacked a "written document retention policy," permitted destruction of evidence by a computer crash, and made material misrepresentations to the court
- Court concluded defendants' behavior added up to a "reckless disregard for their discovery obligation."

Electronic Discovery Disasters

- **Best Practices**

- Attorneys and clients must work together.
- Both must understand how and where electronic documents are maintained.
- Determine how best to locate, review and produce responsive documents.
- Responsibility for production must be determined early and remain clear throughout.

Reasonably Accessible Data

***Aubuchon Co., Inc. v. BeneFirst, LLC*, 245 F.R.D. 38 (D. Mass. 2007)**

- Medical claim forms requested by Plaintiff were not reasonably accessible.
- Original claim forms and medical bills were processed by hand, kept for 60 days, converted to a digital image and then destroyed

Reasonably Accessible Data

Fed. R. Civ. P. 26(b)(2)(B)

- "A party need not provide discovery of electronically stored information from sources the party identifies as not reasonably accessible because of undue burden or cost."
- However, "the court may nonetheless order discovery from such sources if the requesting party shows good cause."
- "The court may specify conditions for the discovery."

Reasonably Accessible Data

Aubuchon Co., Inc. v. BeneFirst, LLC

- Seven-factor approach used to evaluate whether plaintiffs proved that "good cause" existed to compel production
- Court ordered production of the digital images because, *inter alia*, they were not available through any other source.

Reasonably Accessible Data

***Petcou v. C.H. Robinson Worldwide, Inc.*, 2008 WL 542684 (N.D. Ga. 2008)**

- Cost of retrieving about two years' worth of e-mails for one of defendant's employees was approximately $79,300
- Defendant met its burden of showing that deleted emails were not reasonably accessible due to undue burden and cost
- Defendant not required to search its back-up tapes

Reasonably Accessible Data

***John B. v. Goetz*, 2008 WL 2520487 (6th Cir. 2008)**

- Lower court ordered plaintiffs' computer expert - accompanied by deputy U.S. Marshals - to enter state agencies, and the offices and homes of state officials.
- Permitted to make forensic images of hard drives and other devices, whether state-owned or privately owned.

Reasonably Accessible Data

Parkdale Am., LLC v. Travelers Cas. and Sur. Co. of Am., Inc.

- Amount in controversy = $2.7 million and cost of conversion was estimated at only $20,000
- Plaintiffs ordered to convert emails into a searchable format because cost was relatively low and emails contained relevant information to pivotal issues in the case
- Court stated that it could arrange a cost-sharing agreement if necessary

Reasonably Accessible Data

John B. v. Goetz

- Circuit Court stayed lower court's order because of failure to properly account for the significant privacy and confidentiality concerns
- Such procedures, if at all appropriate, should be employed in a "very limited set of circumstances" because "litigants are generally responsible for preserving relevant information on their own"

Reasonably Accessible Data

- **Best Practices**

- Work with lawyers (inside and outside) and IT personnel to understand all of the forms in which data is maintained
- Maintain up-to-date documentation of data storage locations
- Determine what sources of information are reasonably accessible, and which ones aren't

ESI Authentication

***Lorraine v. Markel Am. Ins. Co.,* 2007 U.S. Dist. LEXIS 33020 (D. MD. 2007)**

- Routine dispute over authority of arbitrator to limit damages to boat struck by lightning
- Parties filed summary judgment motions, but did not supply authentication for emails attached as evidence to motions

ESI Authentication

Lorraine v. Markel

- U.S.M.J. Grimm penned 101-page opinion – a primer on admissibility of electronically stored evidence
- ESI must be relevant – FRE 401
- ESI authenticity governed by FRE 901 – which is "silent" on how to authenticate electronically stored document

ESI Authentication

Lorraine v. Markel

- Extrinsic evidence can be used – examples:
- *Testimony of witness with knowledge about storage*
- *Hash marks & metadata*
- *Circumstantial evidence - such as the presence of party's work e-mail address and use of the party's nickname in the e-mail*

ESI Authentication

Lorraine v. Markel

- Self-authentication can be used – examples:
- *Official publication – such as U.S. Govt. website*
- *Inscriptions, signs, tags, or labels – i.e., identification of employer company*
- *Regularly conducted business – i.e., business record exception requirements*

ESI Authentication

Lorraine v. Markel

- Alternate methods of authentication – examples:
- *Judicial notice*
- *Request opposing party to admit genuineness of document FRCP 36*
- *Stipulation between parties*

ESI Authentication

- **Best Practices**
  - Employ proper data collection methods in litigation
  - Designate employee with knowledge who can testify about information technology systems
  - Implement comprehensive records retention policy

HOT TOPICS IN ELECTRONIC DISCOVERY

ELECTRONIC DISCOVERY DISASTERS

- Qualcomm, Inc. v. Broadcom, Corp., 2008 U.S. Dist. Lexis 911 (S.D. Calif. Jan. 7, 2008)
  - The court found that the plaintiff and its outside counsel deliberately failed to produce key documents in connection with the deposition of their corporate representative witnesses. The court imposed sanctions on Qualcomm of more than $8.5 million and reported its attorneys to the state bar.
  - During this patent infringement action, Qualcomm contended that it did not participate in a particular standard-setting process, which – if revealed – would have prevented Qualcomm from suing Broadcom for using a standard adopted by that process. However, when one of Qualcomm's attorneys was preparing a Qualcomm witness, the attorney discovered an email to the witness from the group setting the relevant standard. Instead of producing this email and searching for others like it, Qualcomm and its attorneys decided not to take further action and crafted their discovery responses and deposition testimony to avoid revealing the existence of the emails.
  - The existence of the relevant email was revealed by a Qualcomm employee on the witness stand. Ultimately, the court found that "Qualcomm intentionally withheld tens of thousands of decisive documents from its opponent in an effort to win this case and gain a strategic business advantage over Broadcom." As a result, the court sanctioned both Qualcomm and its outside counsel. The court concluded that "Qualcomm had the ability to identify its employees and consultants who were involved in the [standard-setting process], to access and review their computers, databases and emails, to talk with the involved employees and to refresh their recollections if necessary, to ensure that those testifying about the corporation's knowledge were sufficiently prepared and testified accurately, and to produce in good faith all relevant and requested discovery," but chose not to do so.
- In re Intel Corp. Microprocessor Antitrust Litig., 2008 WL 2310288 (D. Del. 2008)
  - Intel's ESI preservation activities did not, *inter alia*, include suspension of the "auto delete" function of its email system – which automatically deleted emails remaining in an employee's mailbox after 35 days. Intel relied upon individual employees to identify, segregate and move relevant evidence to storage or their local computer before that data was destroyed by a network purge.
  - However, there were lapses in Intel's email retention plan – which an adversary described as a "move-it-or-lose-it 'honor system.'" Intel claimed that its retention lapses were the result of human error and not the result of deliberate deletion. In support of this contention, Intel filed summaries of the causes of its document retention lapses with the court. Intel's summaries were based on its outside attorneys' interviews of more than 1000 employees concerning compliance with their evidence preservation obligations.
  - The court ruled that Intel waived the attorney-client privilege by revealing its understanding of the specific failings of its document retention efforts through the summaries of employee interviews, which were conducted by Intel's outside attorneys.
- Keithley v. The Homestore.com, 2008 WL 3833384 (N.D. Cal. August 12, 2008)
  - Litigation was threatened in 2001. Defendant's chief technology officer testified that a database with the source code in question had been eliminated in 2001 during a transfer to a new system. The CTO also testified that, in 2004, a catastrophic computer failure deleted the code entirely.
  - However, after the plaintiff filed a motion for sanctions – the CTO had "resurgence of memory" and found a backup of the source code. Later that month, an engineer found more of the source code in question in a drawer in her cubicle.
  - As a consequence of this conduct and other spoliation, the defendants were ordered to pay more than $250,000 in monetary sanctions in addition to evidentiary sanctions. The court noted that the defendants lacked a "written document retention policy," permitted destruction of evidence by a computer crash, and made material misrepresentations to the court. The court concluded defendants' behavior added up to a "reckless disregard for their discovery obligation."

Best Practices

- Efforts to save money by reducing the involvement of outside counsel in the process of collecting and producing ESI may be short-sighted. In Qualcomm, the court emphasized that outside counsel has an obligation to supervise the production and is responsible for compliance with discovery obligations.
- Responsibility for production must be determined early and remain clear throughout.
- If outside counsel is not involved at an early stage, then there may need to be duplication of earlier document collection work so that all discovery obligations are met.
- As the Qualcomm court explained, "attorneys and clients must work together to ensure that both understand how and where electronic documents, records and emails are maintained and to determine how best to locate, review, and produce responsive documents."
- Finally, if a party to a lawsuit inadvertently fails to produce information requested in discovery and later discovers such failure, the material should be produced promptly, not concealed.

REASONABLY ACCESSIBLE DATA

Fed. R. Civ. P. 26(b)(2)(B) states that "[a] party need not provide discovery of electronically stored information from sources the party identifies as not reasonably accessible because of undue burden or cost." However, "the court may nonetheless order discovery from such sources

if the requesting party shows good cause." In this regard, "[t]he court may specify conditions for the discovery."

- Aubuchon Co., Inc. v. BeneFirst, LLC, 245 F.R.D. 38 (D. Mass. 2007)
  - The court found that certain digitized medical claim forms in the defendant's possession were not reasonably accessible. However, since the original claim forms and medical bills were processed by hand, kept for 60 days, converted to a digital image and then destroyed, they were not available through any other source.
  - It then evaluated whether the plaintiffs proved that "good cause" existed to compel production of the forms notwithstanding the accessibility issue. The court used a seven-factor approach suggested by the Advisory Committee's note to the 2006 Amendment of Fed. R. Civ. P. 26. These factors are:

    > (1) the specificity of the discovery request; (2) the quantity of information available from other and more easily accessed sources; (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources; (4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources; (5) predictions as to the importance and usefulness of the further information; (6) the importance of the issues at stake in the litigation; and (7) the parties' resources.

  - The court found that good cause existed and ordered production of the requested materials.
- Petcou v. C.H. Robinson Worldwide, Inc., 2008 WL 542684 (N.D. Ga. Feb. 25, 2008)
  - Plaintiffs in an employment discrimination suit sought to compel the production of all email "of a sexual or gender derogatory nature" for a period of eight years.
  - The defendant met its burden of showing that deleted emails were not reasonably accessible due to undue burden and cost. To find responsive emails, the defendant would need to look through email of all of its 5300 employees on backup tapes. The cost of retrieving about two years' worth of e-mails for one of defendant's employees was approximately $79,300.
  - The defendant had already produced reports of attempts by its employees to access adult websites, and it was unclear how defendant could determine what email was "of a sexual or gender derogatory nature" without reviewing each email. Accordingly, the court ordered production only of responsive email of selected employees of the defendant. No search of backup tapes was required.
- Parkdale Am., LLC v. Travelers Cas. and Sur. Co. of Am., Inc., 2007 WL 4165247 (W.D.N.C. Nov. 19, 2007)
  - In this insurance coverage dispute, the amount in controversy was $2.7 million and the cost of converting email into a searchable format was estimated at only $20,000. The court ordered the plaintiffs to convert the emails into a searchable format because the cost was relatively low and the emails contained relevant information to pivotal issues in the case. The court stated that it could arrange a cost-sharing agreement if necessary.
- John B. v. Goetz, 2008 WL 2520487 (6th Cir. 2008)
  - The lower court had ordered plaintiffs' computer expert -- accompanied by deputy U.S. Marshals -- to enter state agencies, and the offices and homes of state officials. The lower court stated that the plaintiffs' expert was permitted to make forensic images of hard drives and other devices, whether state-owned or privately owned.
  - On a request for mandamus relief, the Circuit Court ordered an emergency stay of the lower court's order because of the failure to properly account for the significant privacy and confidentiality concerns. The Circuit Court stated that, such procedures, if at all appropriate, should be employed in a "very limited set of circumstances" because "litigants are generally responsible for preserving relevant information on their own"

Best Practices

- Work with lawyers (inside and outside) and IT personnel to understand all of the forms in which data is maintained.
- Long-term partnerships with outside counsel can help maintain "institutional knowledge" of data sites
- Maintain up-to-date documentation, including detailed system and data schematics, for data storage locations.
- Determine before any litigation commences what sources of information are reasonably accessible and which ones are not, and document the reasons for these determinations.

ESI AUTHENTICATION

- Lorraine v. Markel Am. Ins. Co., 2007 U.S. Dist. LEXIS 33020 (D. MD. 2007)
  - In this routine dispute over the authority of arbitrator to limit damages to boat struck by lightning, the parties filed summary judgment motions, but neither side supplied authentication for emails attached as evidence to motions.
  - U.S.M.J. Grimm penned a 101-page opinion, which is effectively a primer on the admissibility of electronically stored evidence.
  - The decision notes that ESI authenticity is governed by FRE 901 – which is "silent" on how to authenticate electronically stored document. As a general matter, extrinsic evidence can be used to authenticate ESI; for example, the testimony of witness with knowledge about storage of the ESI, or hash marks and metadata. In addition, circumstantial evidence can be used to authenticate ESI, such as the presence of party's work e-mail address and use of the party's nickname in the e-mail. Moreover, alternate

methods of authentication include a Rule 36 admission by a party that a document is genuine or a stipulation between parties as to the same.

Best Practices

- Employ proper data collection methods in litigation
- Designate employee with knowledge who can testify about information technology systems
- Implement comprehensive records retention policy
- To protect important evidence, be prepared to explain through an affidavit, deposition or live testimony:

  The company's policies and procedures for the use of the computer equipment, databases and programs;

  How access to the database and computers are controlled;

  How changes in the database are logged or recorded; and

  The structure and implementation of backup systems and audit procedures.

- Request a stipulation from opposing counsel or propound RFA to determine which electronic documents will need to be authenticated.

ADDITIONAL SIGNIFICANT DECISIONS

- Columbia Pictures v. Bunnell, 2007 WL 2080419 (C.D. Calif. May 29, 2007)
  - Temporary digital information (server log data) was discoverable, even though it had existed only in a computer's random access memory (RAM) (the contents of which is typically deleted once a computer is turned off). Defendants were ordered to capture and preserve server log data that was temporarily stored in RAM and not otherwise written to a permanent file.
  - The court stated that Rule 34(a) "leaves no room to interpret the Rule to categorically exclude information ... simply because that medium stores information only temporarily."
  - Some practitioners are concerned that this decision opens the door to a larger category of ESI and that corporations may be expected to store vast amounts of "ephemeral" data
- Daimler Truck N. Am. LLC v. Younessi, 2008 WL 2519845 (W.D. Wash. June 20, 2008)
  - In a case where the responding party was "responsive and willing to cooperate" with the requesting party's "reasonable requests," and where there were no allegations that ESI was being destroyed by the responding party, the court rejected the requesting party's demand to copy to copy the contents of the responding party's hard drives. The litigants were direct competitors, so the court permitted the responding party to search its own computers, rather than risk disclosure of trade secrets and privileged information.
- Diabetes Centers of America, Inc. v. Healthpia America, Inc., 2008 U.S. Dist. LEXIS 8362, 2008 WL 336382 (S.D. Tex. Feb. 5, 2008).
  - Producing party faulted for failing to conduct a proper search for relevant emails. The task of searching the party's ESI "was entrusted to a junior associate" who "worked with little or no direction or supervision." And the "search terms used by the associate were inadequate," so the responsive emails were not located by the producing party's attorneys. Nevertheless, no sanctions were awarded because, *inter alia*, the court found that there was "material fault on both sides."
- Ferron v. Search Cactus, L.L.C., 2008 WL 1902499 (S.D. Ohio Apr. 28, 2008)
  - Plaintiff (an attorney) claimed that he received misleading spam. Defendants sought a comprehensive forensics exam of Plaintiff's computers.
  - Plaintiff argued that the request was overbroad because he had preserved the relevant email, and that confidential attorney-client communications would be compromised because he used the computers both personally and professionally. However, the court permitted defendant's forensic expert to inspect the plaintiff's computers, but only after plaintiff's forensics expert removed the plaintiff's confidential information from the hard drives. The court designated both experts to act as officers of the court.
- Johnson v. Wells Fargo Home Mortgage, Inc., 2008 WL 2142219 (D. Nev. May 16, 2008)
  - Plaintiff accused of manufacturing electronic evidence was compelled to produce his computers for inspection. Wells Fargo's forensic expert discovered that the hard drives had been "reformatted and/or reinstalled" during the discovery period. Wells Fargo requested dismissal of Plaintiff's claim as a sanction for spoliation of evidence, but an adverse inference jury instruction was ordered instead.
- Victor Stanley, Inc. v. Creative Pipe, Inc., 250 F.R.D. 251 (D. Md. 2008)
  - Magistrate Judge Paul W. Grimm found that the Defendants waived any privilege or work-product protection for 165 electronically stored documents that were disclosed to the Plaintiff. Defendants argued that the documents were inadvertently produced and, therefore, there was no waiver. The Plaintiffs contended that the Defendants did not "take reasonable precautions by performing a faulty privilege review of the text-searchable files and by failing to detect the presence of the 165 documents, which were then given to the Plaintiff as part of Defendants'" document production.
  - The court faulted Defendants for their improper keyword searches and sampling techniques, noting that "all keyword searches are not created equal; and there is a growing body of literature that highlights the risks associated with conducting an unreliable or inadequate keyword search or relying exclusively on such searches for privilege review. Additionally, the Defendants do not assert that any sampling was done

of the text searchable ESI files that were determined not to contain privileged information on the basis of the keyword search to see if the search results were reliable."

NEW PROPOSED RULE 502 OF THE FEDERAL RULES OF EVIDENCE

- S. 2450--110th Congress (2007): A bill to amend the Federal Rules of Evidence to address the waiver of the attorney-client privilege and the work product doctrine.
  - Passed by U.S. Senate on February 27, 2008.
  - This legislation proposes the addition of a new FRE 502.
  - Under this proposed rule, the inadvertent disclosure of the attorney-client or work product protected material does not operate as a waiver if the holder of the privilege took reasonable steps to prevent the disclosure, and attempted to rectify the inadvertent disclosure in accordance with Rule 26(b)(5)(B) of the Federal Rules of Civil Procedure.
  - The new FRE 502 provides that confidentiality agreements between parties are valid as to the parties, and court orders concerning non-waiver are also valid as to third parties in both state and federal proceedings.