Bingham eDiscovery News

Bingham's eDiscovery Group is pleased to publish our next issue of Bingham eDiscovery News, a newsletter covering recent legal developments on electronically stored information (ESI) and other emerging eDiscovery topics. In this issue, we discuss predictive coding and proportionality, sanctions, adoption of eDiscovery rules by the International Trade Commission and proposed discovery rule amendments to the Federal Rules of Civil Procedure that have been approved for public comment. We also report on some important data security updates from Bingham's Privacy and Security Group, a multidisciplinary practice that helps clients understand and litigate data protection and privacy laws, regulations and standards.

Gary Adler
Practice Co-Leader
eDiscovery Group
gary.adler@bingham.com
T +1.212.705.7803
New York

Brian C. Rocca
Practice Co-Leader
eDiscovery Group
brian.rocca@bingham.com
T +1.415.393.2394
San Francisco

James G. Snell
Practice Co-Leader
Privacy and Security Group
james.snell@bingham.com
T +1.650.849.4882
Silicon Valley

PREDICTIVE CODING AND PROPORTIONALITY

Court Refuses to Require Defendant to Redo Discovery Using Only Predictive Coding

In re Biomet M2a Magnum Hip Implant Prods. Liab. Litig., No. 3:12-MD-2391, 2013 WL 1729682 (N.D. Ind. Apr. 18, 2013)

In this products liability matter, defendant had first used keyword "culling" to reduce the "universe of documents" for review in discovery from 19.5 million to 3.9 million. After removing duplicates, 2.5 million documents remained, which were then reviewed using "technology-assisted review, or predictive coding." Defendant's eDiscovery costs at the time of the decision were approximately $1 million and were expected to total between $2 and $3.5 million. Plaintiffs argued that defendant's "initial use of the keyword approach had tainted the process," and that defendant should have used predictive coding from the outset because it is more accurate than using keyword searches.

The court held the defendant had fully complied with its discovery obligations under the Federal Rules of Civil Procedure. The court could not find that the benefits of the plaintiffs' preferred discovery proposal — the usage of predictive coding on the entire document population — equaled or outweighed the additional burden on, and additional expense to, defendant.

The court also held that ordering the defendant to re-review the documents using predictive coding on the entire document population "sits uneasily with the proportionality standard in Rule 26(b)(2)(C)." The defendant's statistical sampling showed that only "a comparatively modest number of documents would be found" by plaintiffs' preferred method. As such, the burden of further searching outweighed the benefit to the plaintiffs: "[i]t might well be that predictive coding, instead of a keyword search, at Stage Two of the process would unearth additional relevant documents. But it would cost [defendant] a million, or millions, of dollars to test [plaintiffs'] theory that predictive coding would produce a significantly greater number of relevant documents."

Keyword Searches Performed with Proper Search Terms will Meet the Standard of a Reasonable Search and Diligent Inquiry

Fosamax/Alendronate Sodium Drug Cases, No. JCCP 4644 (Orange Co. Sup. Ct. Apr. 18, 2013)

The defendants in this products liability case initially used a keyword search to identify and produce relevant documents. Plaintiffs wanted the defendants to search again using predictive coding technology. Like *Biomet*, defendants argued that its search term process constituted the "reasonable search" and "diligent inquiry" required by California rules of procedure. The court agreed in a short minute order, finding plaintiffs could not show that the additional benefit from a new predictive coding search process and ensuing production outweighs the burden on the defendants.

***

The message from *Biomet* and *Fosamax* is proportionality: As courts continue to refine their positions on predictive coding, they will continue to consider reasonableness and efficiency and balance the cost of predictive coding against the benefits of potentially finding relevant documents.

SANCTIONS

Court Rejects Request for Adverse Inference Where Deleted Call Recordings Would Not Have Supported Plaintiff's Claim

Cottle-Banks v. Cox Commc'ns, Inc., No. 10cv2133-GPC (WVG), 2013 WL 2244333 (S.D. Cal. May 21, 2013)

Plaintiff's putative class action complaint alleged the defendant violated the federal Cable Act by failing to disclose and obtain customers' consent to monthly rental fees associated with cable set-top boxes. Plaintiff filed a motion for spoliation sanctions relating to recorded telephone calls between defendant's customer services representatives and its customers. Defendant maintained the recordings for 45 days and then overwrote them, as there was no business need for calls older than 45 days, and retaining calls for a longer period would be costly.

In June 2011, plaintiff sought production of customer call recordings. Plaintiff asserted the defendant had failed to preserve those recordings and continued to "routinely" tape over them. Defendant asserted that the call recordings were on a constant 45 re-recording cycle, that any calls with plaintiff in 2008 were "long gone before the case was filed," and that the calls would not be discoverable under the Federal Communications Act. Defendant had only begun preserving backup tapes containing call recordings in June 2011, when plaintiff put defendant on notice that she would be seeking call recordings in discovery. In response to a motion to compel filed by plaintiff regarding the call recordings, the court ordered defendant to produce a random selection of calls. From the 280 calls produced, plaintiff identified two that supported her claims.

Upon plaintiff's motion for spoliation sanctions, the court examined the three factors necessary to support an adverse inference sanction: "(1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) that the records were destroyed 'with a culpable state of mind'; and (3) that the evidence was 'relevant' to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense." While the court found that the defendant did not preserve potentially relevant customer call recordings at the time the duty to preserve arose (when the complaint was filed in September 2010) it did not order sanctions because plaintiff could not show that the call recordings supported her claims. In making

this finding, the court found highly persuasive that only two of the 280 calls already produced supported plaintiff's position. The court also denied the motion for spoliation on the alternative ground (not raised by the parties) that it had not been timely filed.

This case underscores that allegedly lost evidence is by itself insufficient to secure sanctions against a party. Courts evaluate the nature of the lost material in part by examining available evidence and drawing reasonable inferences about what may be contained in the missing evidence.

Employee Plaintiff's Request for Adverse Inference Granted due to Employer's Failure to Prevent Automatic Deletion of Employee Performance Data

Pillay v. Millard Refrigerated Servs., Inc., No. 09 C 5725, 2013 WL 2251727 (N.D. Ill. May 22, 2013)

In this employment dispute, plaintiff alleged he was terminated because he opposed the termination of another employee. The defendant company asserted it terminated plaintiff for poor performance, which was supported by productivity and performance data tracked by defendant's computerized Labor Management System (LMS). Plaintiff asserted that defendant's LMS rating could have been manipulated by defendant.

Before filing his lawsuit, plaintiff sent a demand letter that placed the defendant on notice of the impending lawsuit. Later, plaintiff sent a preservation notice to defendant's general counsel.

In the course of discovery, defendant informed plaintiff that the LMS software had automatically deleted the underlying data regarding plaintiff's performance because defendant only retained the data for a year to optimize the performance of the LMS system. However, both the demand letter and preservation notice were sent to defendant before the automated deletion of plaintiff's LMS data.

The court found that the pre-filing correspondence with the defendant (along with the filing of additional employment charges) had triggered defendant's duty to preserve. The court also rejected the defendant's assertion that the deleted information was not relevant, noting that the "inquiry is whether this information is the type that would have been discoverable under Rule 26" — which it would have been.

The court therefore granted plaintiff's motion for adverse inference instruction because the defendant had failed to prevent the automatic deletion of relevant data despite notice of reasonably anticipated litigation, including the specific preservation notice sent directly to defendant's general counsel.

This case should remind parties that they may need to suspend automatic data deletion policies or otherwise take steps to preserve data subject to automatic retention policies when the duty to preserve is triggered and where the evidence subject to deletion is potentially relevant to the litigation.

DISCOVERY RULES

U.S. International Trade Commission Adopts eDiscovery Rules

The U.S. International Trade Commission has adopted final rules related to its eDiscovery practices. The new rules are applicable to investigations instituted after June 20, 2013.

The rules address numerous eDiscovery issues, including the discovery of inaccessible information and limitations to discovery similar to those found in Fed. R. Civ. P. 26(b)(2)(C). The newly adopted rules also add new provisions addressing privileged information and work product, including

requiring the production of privilege logs and providing procedures for addressing the inadvertent production of privileged materials.

The rules can be found here.

Proposed Discovery Rule Amendments to the Federal Rules of Civil Procedure Approved for Public Comment

On June 3, 2013, the Standing Committee on Rules of Practice and Procedure of the Judicial Conference of the United States voted to approve for public comment the full slate of proposed amendments to the Federal Rules of Civil Procedure that the Advisory Committee on Civil Rules previously approved on April 12, 2013.

The most significant of the proposals would: narrow the scope of discovery under Rule 26; impose or reduce numerical limits on written discovery and depositions under Rules 30, 31, 33 and 36; tighten the rules governing responses to requests for production of documents under Rule 34; and adopt in Rule 37 a uniform set of guidelines concerning the imposition of sanctions when a party fails to preserve discoverable information.

The Advisory Committee anticipates a high level of public interest in the proposals and plans to hold public hearings in several cities around the U.S.

Any amendment to the Federal Rules of Civil Procedure may have a significant impact on eDiscovery. The public commentary period is scheduled to last until February 15, 2014. A copy of the proposed rules approved for public comment is available here. We will keep you updated on important developments in future issues of eDiscovery News.

DATA SECURITY

There have been several recent state and federal developments regarding privacy and security that may affect corporate data retention practices. In February 2013, President Obama issued Executive Order 13636 on Improving Critical Infrastructure Cybersecurity. The Executive Order directs the U.S. Commerce Department's National Institute of Standards and Technology ("NIST") to develop a Cybersecurity Framework to help organizations evaluate their preparedness against cyber threats. NIST issued a draft of this Framework in early July 2013, which outlines four major sections, including: (1) a guide for senior executives and others on how to use the Framework to evaluate and manage their organizations' cyber risk preparedness; (2) a user's guide for more detailed implementation of the Framework; (3) the "core" structure" of the Framework; and (4) a compendium of references such as existing cybersecurity standards, guidelines and practices. The "core" is currently a blank shell, which NIST expects owners and operators of critical infrastructure and other stakeholders to populate. This set of best practices would include taking a high-level, overarching view of an organization's management of cybersecurity risk, focusing on key functions of the organization's approach to security. While the draft Framework is voluntary and characterized as a guide rather than a manual, it is possible that the final Cybersecurity Framework could become a basis for legislation or be cited in litigation or agency enforcement actions.

NIST also recently published a set of Guidelines for Managing the Security of Mobile Devices in the Enterprise ("Guidelines"). The Guidelines, which update previous NIST guidelines regarding cell phone and PDA security, are designed as a set of best practices for federal agencies to manage and secure employees' mobile devices such as smart phones and tablets. The Guidelines recommend the use of a centralized mobile device management solution for managing the security of both organization-provided and personal mobile devices. Other recommendations include: (a) use of a

documented mobile device security policy that, among other things, defines the type of enterprise resources and mobile devices permitted to access them (and at what level); (b) development of system threat models; (c) designing and acquiring security solutions that provide the necessary services for an organization; (d) testing and implementing security solutions before putting them into production; (e) fully securing each organization-issued mobile device before allowing access; and (f) regularly maintaining mobile device security through operational processes such as deleting or revoking access to risky applications; scrubbing sensitive data before re-issuing devices; deploying upgrades and patches; and performing periodic assessments to confirm that policies, processes and procedures are followed.

State agencies and attorneys general have also shown increasing interest in how businesses manage data security and data breaches. For example, California was the first state to require notifications following a data breach, and in 2012, began requiring certain companies and government agencies to submit copies of these notices to the state Attorney General. California Attorney General Kamala Harris gathered that information and issued a Data Breach Report on July 1, 2013. The Report addresses several key findings, including the fact that more than half of the breaches reportedly resulted from intentional intrusions by outsiders or by unauthorized insiders, while the remaining 45 percent were "largely the result of failures to adopt or carry out appropriate security measures." The Report makes several recommendations, including: (a) the use of encryption when moving or sending digital personal information out of a secure network; (b) tightened security controls on personal information, including training; (c) improved readability for breach notices; and (d) the offering of mitigation products or information on security freezes to victims of breaches involving Social Security or driver's license numbers. The Report confirms that "[t]he Attorney General's Office will make it an enforcement priority to investigate breaches involving unencrypted personal information, and encourage our allied law enforcement agencies to similarly prioritize these investigations."

Other states have also shown increasing interest in issues of cybersecurity. The New York State Department of Financial Services recently sent letters to the largest insurance companies that it regulates, launching an inquiry into policies and procedures relating to cyber attacks. The DFS seeks a wide variety of information, including any cyber attacks suffered by a company in the past three years, as well as the company's cybersecurity safeguards and IT management policies, resources dedicated to cybersecurity, and governance and internal control policies related to cybersecurity. New York Governor Andrew Cuomo has also created a Cyber Security Advisory Board charged with advising on cybersecurity developments and making recommendations for protecting the state's critical infrastructure and information systems. These developments reinforce the importance of maintaining robust data security practices and policies for responding to threats or breaches.

***

This issue of *Bingham eDiscovery News* was prepared by Peter Pound, Courtney Smith and Lyndsey Marcelino.

BINGHAM

Circular 230 Disclosure: Internal Revenue Service regulations provide that, for the purpose of avoiding certain penalties under the Internal Revenue Code, taxpayers may rely only on opinions of counsel that meet specific requirements set forth in the regulations, including a requirement that such opinions contain extensive factual and legal discussion and analysis. Any tax advice that may be contained herein does not constitute an opinion that meets the requirements of the regulations. Any such tax advice therefore cannot be used, and was not intended or written to be used, for the purpose of avoiding any federal tax penalties that the Internal Revenue Service may attempt to impose.