The following is a compendium of articles and case law that may be of interest to our AG offices that are dealing with electronic discovery issues. Neither the National Association of Attorneys General nor the National Attorneys General Training & Research Institute expresses a view neither as to the accuracy of the articles nor as to the position expounded by the authors of the hyperlinked articles.

NOVEMBER 2015

Sedona Releases Final Privacy & Security Commentary

The Sedona Conference released the final version of *The Sedona Conference Commentary on Privacy and Information Security: Principles and Guidelines for Lawyers, Law Firms and Other Legal Service Providers*. This version reflects changes made after the release of its public comment version earlier this year. The Commentary confronts the challenges to privacy and security brought about by new technologies and the sharing of information to conduct business. It provides a framework for addressing information privacy and security concerns in the legal arena and recommends steps that members of the legal community should consider to safeguard the private and confidential information they maintain on behalf of their clients, third parties and their own organization. The Commentary may be downloaded at [http://www.thesedonaconference.org](http://www.thesedonaconference.org).

Ethics Rule on Metadata Proposed in New Jersey

The Working Group on Ethical Issues Involving Metadata in Electronic Documents proposed a change to New Jersey's ethics rules under which attorneys who receive electronic documents would be permitted to review the unrequested metadata, providing that the receiving lawyer reasonably believes the metadata was not inadvertently sent. In its *Report and Recommendation to the Supreme Court*, the Working Group further recommended the following change to Rule of Professional Conduct 4.4(b):

“A lawyer who receives a document or electronic information and has reasonable cause to believe that the document or information was inadvertently sent shall not
read the document or information or, if he or she has begun to do so, shall stop reading it. The lawyer shall (1) promptly notify the sender, and (2) return the document or information to the sender and, if in electronic form, delete it and take reasonable measures to assure that the information is inaccessible."


How to Avoid the Problems of BYOC

The title of this article is not a typo, although the problems of Bring Your Own Device (BYOD) have been widely discussed. While many organizations are still weighing the benefits and risks of BYOD, Bring Your Own Cloud (BYOC) has arrived, which is defined as departments, workgroups or employees owning and controlling public or third party cloud services for storing information. While the advantages of allowing use of a personal cloud at work are cited as efficiency, a more cost-effective system of sharing data and greater access to organization information, the risks to data security and confidentiality are enormous. Those risks are discussed by Michelle Lange of Kroll Ontrack in Avoiding the Dangers of Bringing Your Own Cloud in E-Discovery, which can be accessed at http://www.law.com/sites/articles/2015/10/12/avoiding-the-dangers-of-bring-your-own-cloud-in-e-discovery/.

Caselaw: 30(b)(6) Witness Must Be Prepared and Knowledgeable

Rembert v. Cheverko, 2015 U.S. Dist. LEXIS 152219 (S.D.N.Y. Oct. 9, 2015), deals with a civil suit filed by Paul Rembert, an inmate in the Westchester County Department of Corrections system (“the Department”), over failure to properly treat his fractured arm. Rembert sought emails between prison staff about him, and after three months with no response, Department counsel stated they did not have any such emails. Rembert pressed, and Department counsel finally admitted they had not searched for any emails, promising to initiate a search and still failing to do so, although five Department witnesses confirmed they used email to communicate about patients. Rembert moved to compel, and the Department responded with a small production of emails which Rembert found incomplete. Rembert sought a 30(b)(6) deposition; the Department moved to strike, which was

pg. 2
denied. After the deposition took place, Rembert moved for a properly prepared and knowledgeable 30(b)(6) witness. In reviewing the transcript of the 30(b)(6) deposition that ensued, the court found that the witness was not prepared and had only met with Department counsel for one hour, despite counsel’s assurances to the contrary. The witness did not know the email platform used, whether emails were maintained on the Department’s server or whether their storage was cloud-based, whether there were any size constraints on the amount of email a user could retain and a host of related issues. The court granted the motion, and ordered the Department to pay Rembert’s costs in bringing the motion, as well as reasonable attorney’s fees for attending the first deposition and attendant court reporter fees.

**Caselaw: No Spoliation Sanctions Absent Evidence of Prejudice**

In *West v. Talton*, 2015 U.S. Dist. LEXIS 147955 (M.D. Ga. Nov. 2, 2015), Rick West had brought an employment discrimination suit against his former employers, Houston County, Georgia; Sheriff Cullen Talton and Major Charles Holt of the Sheriff’s Department, claiming he was terminated on the basis of his race. During a deposition of a County employee, West learned that defendants failed to search and preserve email accounts as requested; that backup tapes of the County’s server were written over; and that Holt’s email account was deleted soon after his resignation. Specifically, the County’s server was backed up every six months, which erased any backup of Holt’s email account. However, West was still able to retrieve Holt’s old computer and hire a third party to preserve and search its hard drive. Both parties were then able to search Holt’s email, and West recovered more than 1,000 emails to support his claims. West sought a spoliation instruction to the jury regarding the deletion of emails or, alternatively, an opportunity to present evidence to the jury of the County’s failure to preserve emails. The County moved to exclude any argument or evidence of spoliation by West, arguing that the emails were not deleted in bad faith, and West still obtained the evidence from Holt’s hard drive. The court granted the County’s motion, determining that Holt’s emails were deleted as part of a routine procedure to delete an employee account after an employee left, and finding the failure to preserve was more “mere negligence” than spoliation. The court concluded that West failed to establish
prejudice, so the court determined a sanction was inappropriate. The court also cited FRE 403, reasoning that it found "the danger of confusing issues and misleading the jury outweighs the probative value of such evidence."

**MD Ct of Appeals: Serial Abuse of Discovery Warrants Disbarment**

In *Attorney Grievance Commission v. Mixter*, 441 Md. 416 (2015), consisting of 130 pages, the Maryland Court of Appeals determined that Mark Mixter violated the rules of discovery so "flagrantly, repeatedly and relentlessly" that he should be disbarred. The court found that in 22 cases and over a period of approximately seven years, Mixter abused the rules of subpoenas; made frequent misrepresentations in motions to compel and for contempt; frequently noted depositions in the wrong venue; failed to make good faith attempts to resolve discovery disputes and then lied about it; misrepresented the contents of court orders; and misrepresented the terms of expert witness compensation. The case can be accessed at [http://bit.ly/441-md-416](http://bit.ly/441-md-416).

**Identifying Duplicates: Consider Message Thread Analysis**

Identifying duplicates can create one of the biggest problems in reviewing ESI. Not only is it costly for reviewers to look at the same documents twice, but there is also the danger of a document being categorized differently by different reviewers. As many of you know, exact duplicates can be identified by using hash values (deduplication through hashing), with MD5 and SHA being the most widely used hashing algorithms, and then removed from the review. However, sometimes files can be exact in content but not in format, such as a Word file published to an Adobe pdf file. Many of you use near-deduplication, a feature in many software platforms, which can be used to identify these files, enabling them to be verified and then eliminated from the review. Another method of identifying duplicates to consider, particularly with emails, is message thread analysis. Many email messages are part of a larger discussion. Reviewing each email in the discussion thread would involve in a great deal of the same information being reviewed again and again, so message thread analysis, which are part of several review platforms, gathers these messages together and enables them to be reviewed as an entire discussion. The software will also include side conversations which potentially might (or might not)
be related to the original subject. The result enables you to focus your review often on the last emails in each conversation.

**Article: Protecting PII in E-Discovery**

A new article in the Westlaw Computer and Internet Journal, *Mission Impossible: Securing Rogue Personal Information in E-Discovery*, discusses the challenges of finding and removing personally identifiable information (PII) during discovery. For example, PII may be contained in a collection of data from human resource records in employment cases and may also be unintentionally included in an overly broad collection. As noted in the article, a recent study revealed that more than one billion PII records were disclosed in 2014. The article may be accessed at [http://www.ediscovery.com/cns/pdf/WLJ_CMP_3308_Commentary_Loveall.pdf](http://www.ediscovery.com/cns/pdf/WLJ_CMP_3308_Commentary_Loveall.pdf).

Hedda Litwin is the Editor of the E-Discovery Bulletin and may be reached at 202-326-6022.

The E-Discovery Bulletin is a publication of the National Association of Attorneys General.

Any use and/or copies of this newsletter in whole or part must include the customary bibliographic citation.

NAAG retains copyright and all other intellectual property rights in the material presented in this publication.

NAAG, 2030 M Street, NW, Eighth Floor, Washington, DC 20036