Monday, October 1, 2012
11:00 AM - 12:30 PM

1001 – Defensible Records Retention Planning

Robert Jett
VP, Deputy Compliance Counsel
RGA Reinsurance Company

Jeffrey Stredler
Senior VP, Litigation Counsel
Amerigroup Corporation

George Tziahanas
Senior Vice President, Legal and Compliance Solutions
Autonomy, an HP Company

Faculty Biographies

Robert Jett

Robert S. Jett III is vice president, deputy compliance counsel and corporate data privacy officer for RGA Reinsurance Company ("RGA"). Based in the St. Louis global headquarters, he leads and manages the compliance division of RGA's global legal services department.

Mr. Jett has been representing insurance and reinsurance companies for more than 21 years and has dealt with the insurance and reinsurance operations of multi-national insurance organizations in all fifty states, Europe and in other foreign jurisdictions.

Mr. Jett earned his BA in international relations and political science from Hobart College in Geneva, NY, and his JD from the University of Baltimore School of Law. He is a member of the Association of Corporate Counsel; the American Bar Association; and the Maryland State Bar Association. He is also a member of the international baccaleureate advisory board for the School of Business at the University of Missouri St. Louis.

Jeffrey Stredler

Jeff Stredler joined Amerigroup Corporation as its senior vice president and litigation counsel. His responsibilities include handling and overseeing Amerigroup's litigation matters, managing e-discovery and the legal hold process for the company, and advising the company regarding information governance and record retention issues.

Prior to joining Amerigroup, Mr. Stredler was a partner in the Norfolk, VA office of Williams Mullen, where he represented corporate and individual clients in connection with a wide variety of complex civil and criminal cases.

Mr. Stredler currently serves on the Virginia State Bar litigation section board of governors and the Virginia State Bar corporate counsel section board of governors. He has also served as the president of the Norfolk & Portsmouth Bar Association, as well as on the boards of directors for the Make-A-Wish Foundation of Eastern Virginia, the Girl Scout Council of Colonial Coast, and the Virginia Beach and Norfolk divisions of the Hampton Roads Chamber of Commerce. He received the Norfolk & Portsmouth Bar Association's Community Service Award in 2003 and the Virginia Beach Bar Association's Community Service Award in 2004.

Mr. Stredler graduated from the University of Virginia and the University of Virginia School of Law.

George Tziahanas
Senior Vice President, Legal and Compliance Solutions
Autonomy, an HP Company

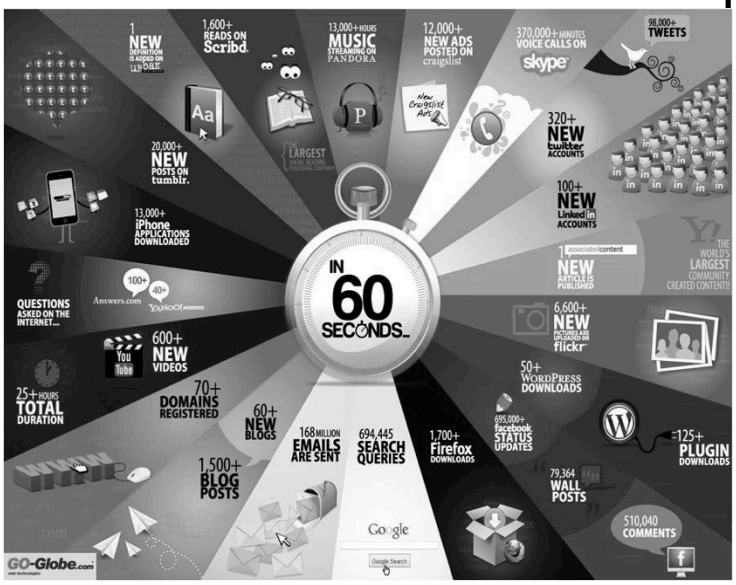
Session 1001

Defensible Records Retention Planning

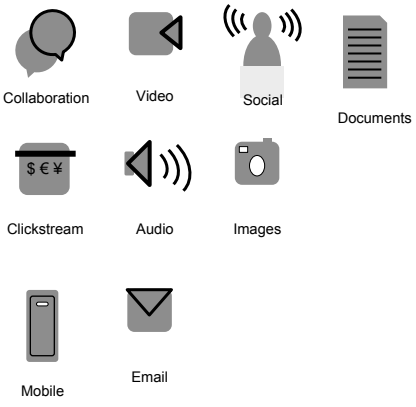
•Defensible Disposition

•George T. Tziahanas
•SVP Legal and Compliance Solutions

The New Information Landscape

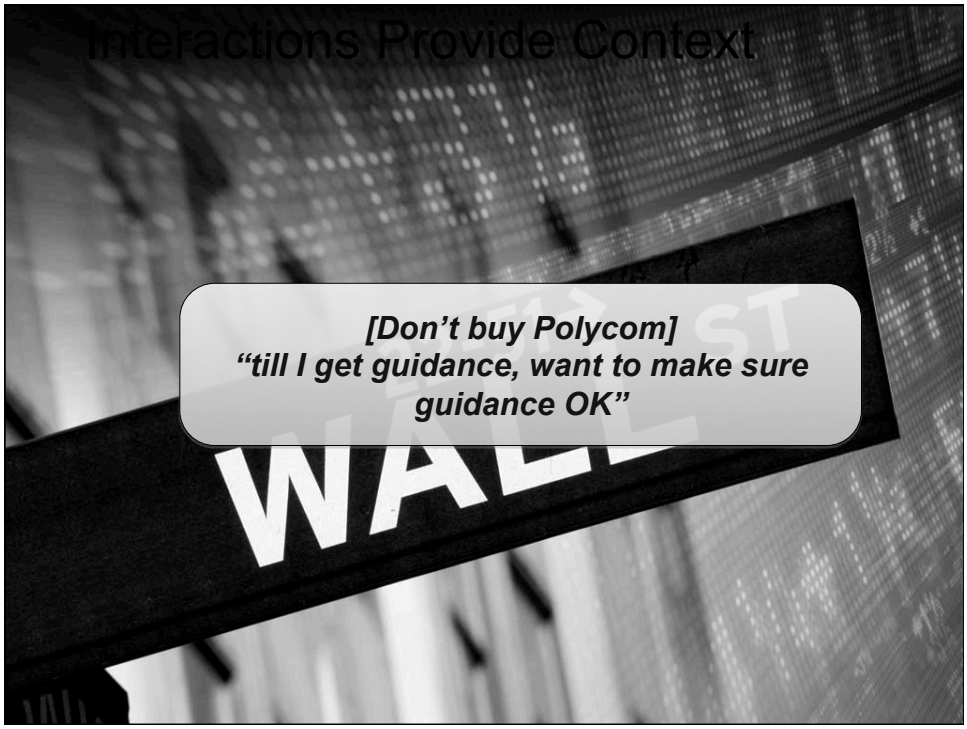


Human Information



Human Information

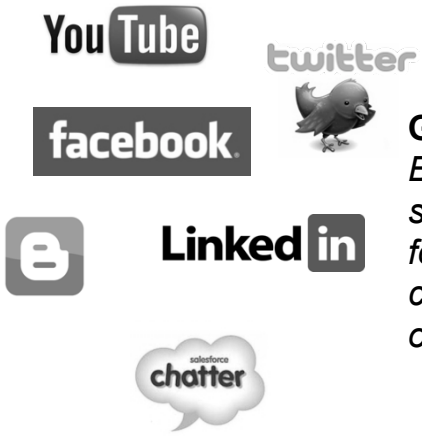
	Amount	Growth
Unstructured	**90%**	**62%**
Standard	10%	22%



Key Trends --- Internal Blurs with External

With the increased blurring of internal and external data – more organizations are using data outside firewall to drive their business

Key Trends --- Social in the Workplace



Gartner's prediction:
By 2014, social networking services will replace e-mail as for interpersonal business communications for 20 percent of business users.

Where is the Content? Who Owns the Content?

- Some Content is Inherently Third-Party
  - Increasing amounts of business content is held by a third-party
  - Potentially relevant content may never have traversed corporate networks or devices
- Account and Content Ownership
  - Social media and public cloud account relationships generally exist between an employee and the site
    - Enterprise may have **no privity**
  - Content ownership itself may rest with third-party

Privacy Implications: Critical Question

Even if a corporation gains access to all types of "personal" interactions as part of its retention and monitoring for "business" interactions…does it really want them?

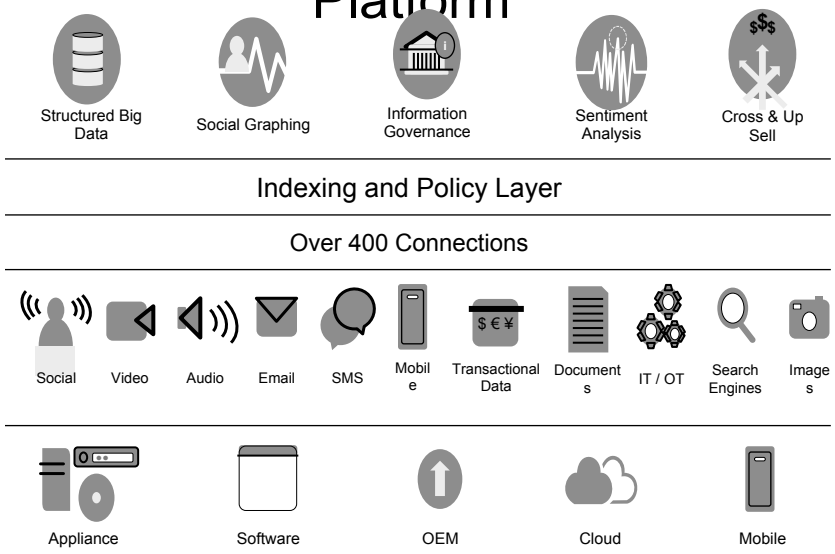
Downside Risks to Personal Interactions in the Enterprise

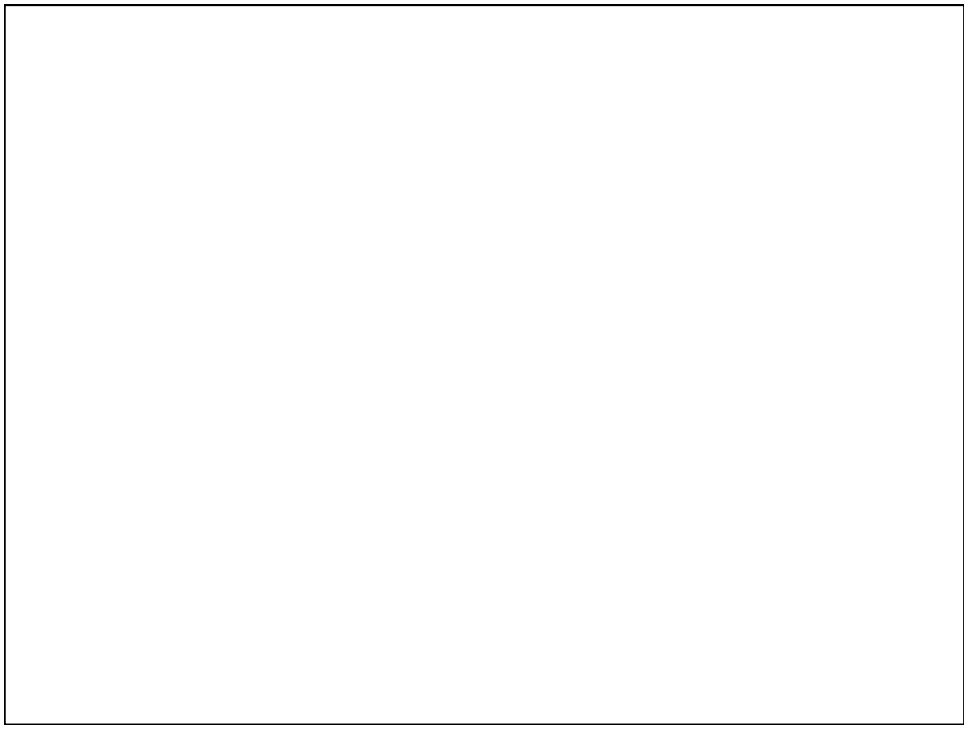
- Assuming legal and lawful access to social media interaction makes "personal" or "non-business" material available to an entity, new risks emerge
  - Enterprises become liable for potential loss of personal or private information
  - Access to personal information that becomes more broad than necessary to meet regulatory requirements
  - Decisions to hire, fire, reprimand, not-promote based on material that is outside the scope of employment, or truly of a personal nature
- Be Careful What You Wish For

Social Media and Cloud-Based Content

- Have a Clear Policy
  - Centralized voice of an organization v. disparate voice of individuals
  - Involve all affected stakeholders in strategic policy planning where possible
- Be Clear About What Will be Captured
  - *Stengart v. Loving Care Agency, Inc.,* 201 N.J. 300, 990 A.2d 650 (2010)
  - *Holmes v. Petrovich Dev. Co LLC,* 2011 Cal. App. LEXIS 33 (Jan 13, 2011)
- Understand What Cannot be Captured
  - Privacy issues related to personal accounts
  - Impact on preservation and collection
- Do Not Suppress Employees, Empower Them

Next-Generation Information Platform





Creating a Defensible Records Management Program

Key Considerations:

- Definition of a “record”
- Policy statement
- Retention schedules
- Records system
- Legal hold protocol/ eDiscovery
- Destruction/ Disposition
- Audit and improvement considerations

Proper Record Retention is Mandated by Numerous Laws and Regulations:

1. Sarbanes – Oxley (SOX)
2. Securities and Exchange Commission (SEC)
3. Internal Revenue Service (IRS)
4. Medicare
5. Health Insurance Portability and Accountability Act (HIPAA)
6. Federal Insurance Contribution Act (FICA)
7. Equal Pay Act/Fair Labor Standards Act/ Americans with Disabilities Act
8. Davis-Bacon Act/Services Contract Act/ Walsh-Healy Public Contracts Act
9. Immigration Reform and Control Act (for INS Form I-9)
10. Occupational Safety and Health Act (OSHA)
11. Toxic Substances Control Act
12. Executive Orders
13. State Laws and Regulations related to licensed buisness activities
14. International Laws

17

Objectives and Definitions

- Developing a shared vocabulary to communicate
- Information is any information, whether in paper, digital or other media, which is recorded and maintained in a form that can be perceived.
- “Records” are information assets that are created and preserved in order to meet legal, compliance and regulatory obligations or to preserve evidence of specific transactions within an organization for historical reference or business continuity management.

Records Management – What is it?

- Systematic controls regarding the creation, receipt, maintenance, use, storage and destruction of records.
- The definition itself suggests that this is an active, continuing process –

  a defensible records management program cannot be achieved by simply placing papers and DVDs in a box with appropriate labeling and moving it to a secure offsite location.

Records Management – What Is It? (2)

Considerations to enhance defensibility:

- *Ownership of the process* – identify the ownership of the policy and define roles
- *Design the policy with flexibility* to respond to changes in the types of "records" produced and maintained
- Employees should be educated and trained regarding the importance of the Records Management Program and their role in making it successful.

Records Management – What Is It? (3)

- The Program must have procedures to provide for the suspension of records destruction in the event of litigation or a government investigation that is reasonably anticipated, threatened, or pending.
  - Destruction of records = allegations of spoliation
  - Could lead to harsh sanctions
  - Inventory of destroyed records
- Documentation and Records pertaining to the development and implementation of the program should be retained.
  - Retention schedules (amendments and updated procedures)
  - Approvals
  - Legal research in support of time periods

21

Insights and Clarifications

- Records are not merely paper documents; records can include electronic versions of paper documents (such as spreadsheets and photos) and electronic files for which no paper equivalent may exist (voicemail and videos).
- A document can be nearly any type of information, and many official regulations include definitions that broaden the scope.
- Electronically stored information ("ESI") has become a formal term to described the use of digital information as evidence in legal proceedings. ESI broadly includes any type of digital asset, whether or not considered a document.
- Drafts and versions of files and/or records may require rules regarding their retention and disposition.

Effective management of records

- Enables Compliance with applicable legal and regulatory requirements
  - Fulfills legal duties to maintain records
  - Preservation and access enhances support for other corporate activities like, contract management, compliance management and production of appropriate records in legal proceedings
- Supports Efficient and responsive business management
  - Vital business information can be located quickly
  - Business planning process is more efficient with access to “historical” information
  - Documentation already gathered or available to support M&A, financial lending or other significant corporate activities
- Enhances business continuity/ disaster recovery planning & response
  - Access to critical records is important

Retention Schedule

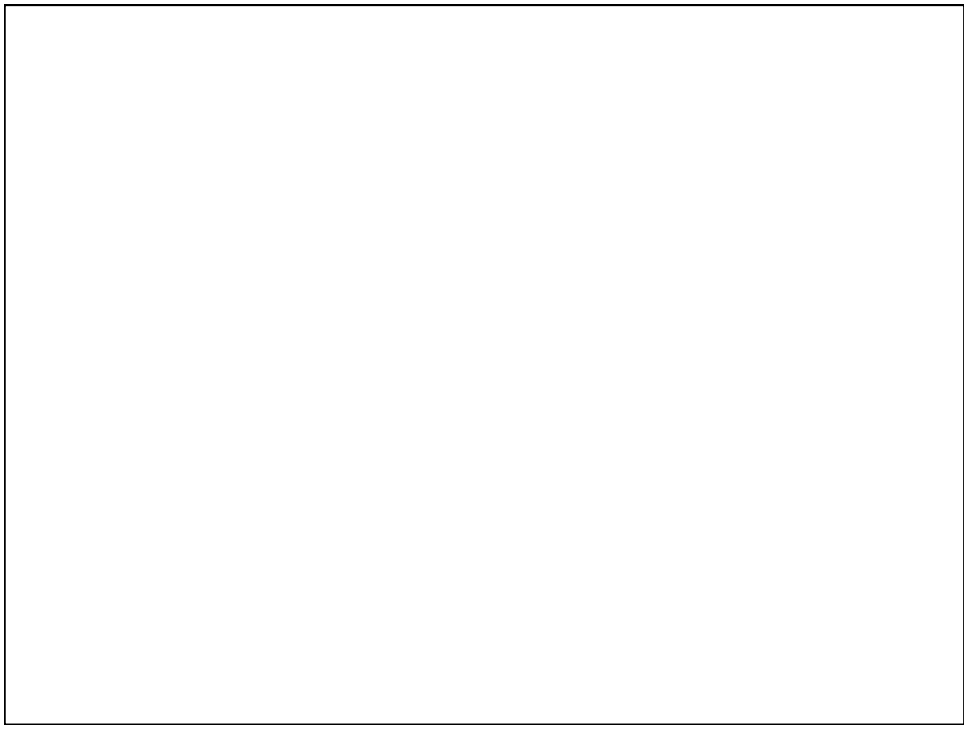
- Critical tool that defines time periods for which a record is retained to meet applicable legal requirements and business needs.
  - Requires active management and monitoring to reflect changes in legal rules, business activities and information retained.
  - Changes should follow a formal documented process
- Retention schedule can also describe the functional rules regarding the maintenance of specific records.
  - Who has access to stored records and why
  - Controls implemented to control and limit access (encryption)
  - Creation of duplicate or backup copies of records
  - Minimum storage quality criteria (e.g. warehouse in a flood zone)

Classification

- Classification of records provides a grouping of the information assets into categories for the various types of records
- Provides common language and consistency
- Promotes efficiencies related to retrieval and disposition

Creating the Program
A quick reference guide

- Create an inventory of existing records systems, including the classifications, retention schedules, and staff involved.
- Develop detailed understanding of the business processes that create the information and records to be managed – include the flow of the information and records
- Document both the legal and the business requirements
- Design the tools to implement and maintain the governance of the records management policy
- *Get rid of the stuff you don't need*. Most companies have obsolescent or historical records which are not required to be retained.



A Defensible Records Retention Program Requires That An Organization Suspend Its Routine Document Retention/ Destruction Policy When Litigation is Reasonably Anticipated Or When A Litigation Hold Is Issued.

- ***Voom HD Holdings LLC v. EchoStar Satellite L.L.C.,*** 93 A.D. 3d 33, 2012 N.Y. App. Div. LEXIS 559 (N.Y.A.D. 1st Dept. Jan. 31, 2012). In this contract dispute, New York's Appellate Division, First Department, adopted the standard for the preservation of electronic evidence as set forth in *Zubulake v. UBS Warburg, LLC*, 220 FRD 212 (S.D.N.Y. 2003). In June 2007, counsel for Echostar sent the plaintiff a letter containing a notice of breach of contract. The plaintiff filed suit in early February 2008, but the defendant did not implement a litigation hold until a later date. It was not until four months after the filing of the lawsuit that the defendant finally took measures to stop the automatic deletion of emails and the plaintiff moved for sanctions. Of significant importance to the trial court was the fact that the **defendant's "purported hold" did not suspend its automatic deletion of emails,** under which any emails sent or

28

deleted by an employee were automatically and permanently purged after seven days. In citing *Zubulake*, the trial court granted the sanctions motion and held that the defendant should have reasonably anticipated litigation and preserved potentially relevant ESI (and ceased the automatic deletion of its e-mails) no later than when it sent its notice of breach letter. The Appellate Division also cited the *Zubulake* decision and upheld the sanctions award as "appropriate and proportionate" a result of the defendant's spoliation of ESI. The trial court noted that the spoliation was "more than negligent" since the defendant had been placed on notice of its "substandard document practices" in another recent lawsuit *(Broccoli v. EchoStar Communications Corp*., 229 F.R.D. 506 (D. Md. 2005).

29

- ***Apple, Inc. v. Samsung Elecs. Co., Ltd.,*** No. C 11-1846 LHK (PSG) (N.D. Cal. July 25, 2012), 2012 U.S. Dist. LEXIS 103958 – In this patent infringement case, Magistrate Judge Paul Grewal granted Apple's motion for an adverse inference jury instruction as a result of, *inter alia*, Samsung's failure to suspend its automatic biweekly destruction of e-mails from its e-mail system. The court mentioned at the outset of its opinion that "Samsung's auto-delete function is no stranger to the federal courts" and cited a previous case (*Mosaid Tech., Inc. v. Samsung Elecs. Co. Ltd.*, 348 F. Supp. 2d 332 (D.N.J. 2004)) in which Samsung was sanctioned with an adverse inference jury instruction and monetary sanctions for spoliation. In addition to its failure to suspend the auto-delete functionality of the e-mail system, the court also ruled that Samsung did not meet its preservation obligations by failing "to issue sufficiently distributed litigation hold notices" after it was apparent that litigation was reasonably anticipated and by not monitoring the preservation efforts of its employees.

30

- ***Passlogix, Inc. v. 2FA Tech., LLC***, 2010 WL 1702216 (S.D.N.Y. Apr. 27, 2010). The plaintiff alleged the defendants, failed to implement a litigation hold which resulted in the spoliation of electronic evidence in this licensing agreement litigation. Despite acknowledging the deletion of Skype and text messages, e-mails, and network and computer logs, the defendants asserted that the electronic evidence was not relevant to the pending case. The plaintiff sought sanctions, including an adverse inference instruction, a ruling that the defendant be prohibited from making arguments implicating the deleted records, and costs. In discussing the sanctions and issue of spoliation, the court noted that a litigation hold must be put in place when litigation is reasonably anticipated and routine document retention and destruction policies must be suspended, which the defendants failed to do in this case. The court ruled that the failure to preserve the text, e-mail, and Skype messages constituted gross negligence and the failure to preserve computer logs was intentional. The court ruled that a $10,000 monetary fine was the appropriate remedy given that the defendant was a small company.

31

- ***Doe v. Norwalk Cmty. Coll.***, 2007 WL 2066497 (D.Conn. July 16, 2007). The plaintiff alleged sexual assault by a professor in this suit brought under Title IX of the Education Amendments of 1972. The plaintiff motioned the court to sanction the defendants for discovery misconduct and spoliation of evidence. The plaintiff claimed that the defendants scrubbed or wiped the hard drives of relevant individuals and altered, destroyed, or filtered relevant data. The defendants denied that their production was insufficient and asserted that scrubbing the hard drives was a normal business practice and therefore they should be protected by the safe harbor of Federal Rule of Civil Procedure 37(f). The court held that in order to take advantage of the good faith exception in the FRCP, a party needs to act affirmatively to prevent the system from destroying or altering information, even if such destruction would occur in the regular course of business. As the defendants failed to suspend their destruction process at any time and the destruction was not due to the routine operation of the information system, the court found the plaintiff was entitled to an award of costs associated with the motion and an adverse jury instruction regarding the destroyed evidence.

32

- ***915 Broadway Assoc., LLC v. Paul, Hastings, Janofsky & Walker, LLP***, 2012 N.Y. Misc. LEXIS 708 (Supreme Court, New York County February 16, 2012) – In an action for professional malpractice, the defendant law firm moved for sanctions based on plaintiff's alleged spoliation of evidence, including the intentional destruction of documents by a representative of plaintiff. In its motion, the firm asked that the case be dismissed with prejudice and that it be awarded its fees and costs incurred in connection with the motion. In granting the motion and dismissing the case, the trial court cited V*oom* and *Zubulake* and stated "[o]nce a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a litigation hold to ensure the preservation of relevant documents." The court also stated "like the contents of a filing cabinet, which must be retained by a party to a pending or reasonably foreseeable litigation, electronic information saved on computers and email servers must also be diligently preserved."

33

- ***State Nat'l Ins. Co. v. Cty. Of Camden***, 2012 WL 960431 (D.N.J. 2012) – District Court upheld Magistrate Judge's Order granting Motion for Sanctions against County for its failure to institute a legal hold and disable its automatic email deletion program.

34

Beware Of The Dangers Inherent In Employee Self-Collection Of Records

- ***Green v. Blitz U.S.A., Inc.***, 2011 WL 806011, 2011 U.S. Dist. LEXIS 20353 (E.D. Tex. Mar. 1, 2011). This was a products liability case in which the plaintiff asked to re-open her settled case and sought sanctions against the defendant for discovery misconduct, including its failure to produce relevant records during the pendency of her underlying case. The documents in question were discovered by counsel for plaintiff nearly a year after trial while conducting discovery in a related matter. The court determined that the subject e-mails should have been produced in the original case and the failure to do so prejudiced the plaintiff. An analysis of this opinion shows that self-collection was one of the major problems with the original document production.

35

The primary individual in charge of collection was closely tied to the research and development of the product in question (a flame arrester). The court also noted "[t]hat Blitz put someone in charge of its discovery who knows nothing about computers does not help Blitz's effort to show that it was reasonable in its discovery obligations." The court found the defendant's discovery efforts were unreasonable because, inter alia, the defendant did not conduct a search of electronic data, failed to institute a litigation hold, instructed employees numerous times to routinely delete information and engaged in other conduct that resulted in the deletion of data. Although the court declined to re-open the case, it ordered the defendant to pay $250,000 in civil contempt sanctions and it imposed a "purging" sanction of $500,000, which was extinguishable if the defendant furnished a copy of the opinion and order to every plaintiff in every lawsuit it has had proceeding against it for the past two years. In addition, the court ordered the defendant corporation to file a copy of its sanctions order with its first pleading or filing in all new lawsuits for the next five years from the date of the order.

36

- ***Nat'l Day Laborer Org. Network v. U.S. Immigration & Customs Enforcement Agency***, 2012 U.S. Dist. LEXIS 97863 (S.D. N.Y. July 13, 2012) - In her fifth decision in this case, Judge Shira Scheindlin addressed the adequacy of self-collection by government entities in the context of the Freedom of Information Act. The plaintiffs made a FOIA request seeking information from five federal agencies regarding the Secure Communities program. Although the government contended that it conducted "massive" searches and produced voluminous records, the requestors challenged the adequacy of the production. Some of the agencies did not monitor custodians but instead allowed them to conduct their own searches to gather information. The court expressed concerns with this approach and emphasized the importance of attorney oversight in the collection process because "most custodians cannot be 'trusted' to run effective searches because designing legally sufficient electronic searches in the discovery or FOIA contexts is not part of their daily responsibilities." The court also referred to its opinion in *Pension Comm. of the Univ. of Montreal Pension Plan v. Banc. Of Am. Sec., LLC,* 685 F.Supp.2d 456 (S.D.N.Y. 2010) in stating the importance of attorney oversight of the process, including counsel's

37

ability to review, sample, or spot-check the collection efforts. Although this opinion involves the reasonability of federal government agency FOIA search efforts and not the somewhat less burdensome discovery requests governed by the Federal Rules of Civil Procedure, it will most likely be cited in future e-discovery disputes.

- ***Northington v. H&M, Int'l***, 2011 U.S. Dist. LEXIS 14366 (N.D. Ill. Jan. 12, 2011) – In this case, the plaintiff sued her former employer for employment discrimination and retaliation in violation of Title VII. The plaintiff filed a motion for sanctions as a result of the defendant's discovery efforts and production. Noting that the defendant's efforts to preserve records were both "reckless and grossly negligent," the court sanctioned the defendant by ordering it to pay attorneys' fees and costs and also allowed for an adverse inference jury instruction regarding the defendant's failure to preserve ESI. One of the primary factors the court considered in finding that the defendant's preservation efforts were unreasonable was the fact that the defendants asked interested custodians to search their own hard drives and documents without supervision or instruction.

39

Other Cases That Address Or Discuss Self-Collection of Records

- ***Ford Motor Co. v. Edgewood Properties, Inc.***, 2009 WL 1416223 (D.N.J. 2009) (opinion discusses *Sedona Conference Best Practices Commentary*).
- ***Pension Comm. Of the Univ. of Montreal Pension Plan v. Banc of America Sec. LLC***, No. 05 Civ. 9016 (SAS), 2010 WL 184312 (S.D.N.Y. Jan. 15, 2010) – The court took exception to a self-collection process that unreasonably placed "total reliance on the employee to search and select what that employee believed to be responsive records without any supervision from counsel."
- ***Jones v. Bremen High School District***, 228, 2010 U.S. Dist. Lexis 51312 (N.D. Ill. May 25, 2010) – The court found

40

defendant grossly negligent in relying on its employees to determine which ESI was relevant for production and which documents could be permanently deleted.

- ***Roffe v. Eagle Rock Energy GP, L.P.***, C.A. No. 5258-VCL (Del. Ch. April 8, 2010) – In this case, the court hearing a discovery dispute informed the attorneys as follows: "[Y]ou do not rely on a defendant to search their own e-mail system… There needs to be a lawyer who goes and makes sure the collection is done properly… we don't rely on people who are defendants to decide what documents are responsive, at least not in this Court." *See* Transcript of telephone conference on discovery dispute at page 10.

41

