International Municipal Lawyers Association
2013 Annual Conference
San Francisco, California

Work Session XIV: Using Cloud Computing to Gain Greater Efficiency

Jeff Arvidson*
Director, New Product Development
Thomson Reuters
Eagan, MN

Peter Haskel
Executive Assistant City Attorney
Dallas City Attorney's Office
Dallas, TX

Matthew Reynolds
IT Director
Meyers Nave
Oakland, CA

©2013 International Municipal Lawyers Association. This is an informational and educational report distributed by the International Municipal Lawyers Association during its 2013 Annual Conference, held September 29 –October 2, 2013 in San Francisco, CA. IMLA assumes no responsibility for the policies or positions presented in the report or for the presentation of its contents.

*Written Materials provided by Jeff Arvidson on behalf of Thomson Reuters

Using Cloud Computing to Gain Greater Efficiency

International Municipal Lawyers Association Annual Conference
San Francisco, CA
October 2, 2013

Table of Contents

The National Institute of Standards and Technology (NIST)
Definition of Cloud Computing ……..…… Page 1

Making the Leap to the Cloud: Is My Data Private and Secure? …….……Page 8

Emerging Legal Technologies and Workflow Challenges
Facing Public Law Offices ..……..……..…… Page 12

Preservation and Legal Holds In the Public Sector ……..…….. Page 16

Thomson Reuters Concourse

- Concourse Matter Room ……..……..……..…. Page 26
- Concourse Legal Hold ……..……..……..…. Page 27

National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-145

The NIST Definition of Cloud Computing

Recommendations of the National Institute of Standards and Technology

Peter Mell
Timothy Grance

NIST Special Publication 800-145

The NIST Definition of Cloud Computing

Peter Mell
Timothy Grance

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

September 2011



U.S. Department of Commerce

Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology

Patrick D. Gallagher, Under Secretary for Standards and Technology and Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-145
7 pages (September 2011)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Acknowledgements

The authors Peter Mell and Timothy Grance of the National Institute of Standards and Technology (NIST) would like to thank the many experts in industry and government who contributed their thoughts to the creation and review of this definition. We especially acknowledge Murugiah Souppaya and Lee Badger, also of NIST, and Wayne Jansen of Booz Allen Hamilton, whose advice and technical insight assisted this effort.

Errata

The following changes have been incorporated into Special Publication 800-145, as of the date indicated in the table.

DATE	TYPE	CHANGE	PAGE NUMBER
4/27/2012	Editorial	Corrected page number from “2” to “1”	1

1. Introduction

1.1 Authority

The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets; but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), "Securing Agency Information Systems," as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority, nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official.

1.2 Purpose and Scope

Cloud computing is an evolving paradigm. The NIST definition characterizes important aspects of cloud computing and is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing. The service and deployment models defined form a simple taxonomy that is not intended to prescribe or constrain any particular method of deployment, service delivery, or business operation.

1.3 Audience

The intended audience of this document is system planners, program managers, technologists, and others adopting cloud computing as consumers or providers of cloud services.

2. The NIST Definition of Cloud Computing

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics**,** three service models, and four deployment models.

Essential Characteristics:

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability[1] at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Service Models:

Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure[2]. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming

[1] Typically this is done on a pay-per-use or charge-per-use basis.

[2] A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.

languages, libraries, services, and tools supported by the provider.[3] The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models:

Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

[3] This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.

MAKING THE LEAP TO THE CLOUD: IS MY DATA PRIVATE AND SECURE?

WHITE PAPER

CLOUD COMPUTING: WHAT'S IN IT FOR ME?

The more you know about cloud computing, the more you'll understand why it has received so much attention in recent years. Also referred to as hosted computing, cloud computing generally refers to a complete software solution that your organization accesses over the Web. Cloud computing provides secure anytime-anywhere access, high-level security and data privacy, and it holds the potential to bring about some of the most far-reaching efficiency and productivity improvements seen by the legal profession. Its benefits include:

- **Reduced costs** – organizations pay incrementally for cloud computing software, saving money and making budgeting easier and more predictable.
- **Safer data** – cloud computing offers an unprecedented level of physical protection against fire, flood, data theft, and other concerns.
- **Anytime/anywhere data access** – you can access hosted data from anywhere, anytime. You can also choose to give your employees any level of access, from full 24/7 access to total lockout.
- **Increased storage capacity** – you can store more data than with on-site hosted servers, and storage capacity is easy to upgrade when needed.
- **Worry-free maintenance** – hardware, software, and security upgrades are handled automatically by professional data center staff. You will always have the latest and most secure technology, with no additional cost or downtime.

Yet, for all its advantages, cloud computing still makes some organizations a little uncomfortable, simply because it requires us to think about our data in a different way. How do we know our data is safe when we can't see it? Can we trust a third party with such important information?

The goal of this white paper is to address those concerns and clarify complexities around the security and privacy of cloud computing solutions. It outlines cloud computing providers and their role in maintaining the privacy of your data. And perhaps most importantly, it offers on-the-ground tips that can help you find the right cloud computing provider.

IS CLOUD COMPUTING SECURE?

If done correctly, yes. In fact, cloud computing offers a level of physical and electronic security that an on-site server or a locked file cabinet can't begin to approach.

Because they can operate with large economies of scale, data centers can be surprisingly affordable, offering even smaller agencies and departments a level of security far beyond what they could achieve on their own. But all data centers are not created equal, so it's important to be sure that the one you choose can adequately protect your data.

The data center you choose should offer the following protection measures:

PHYSICAL SECURITY

- **Redundant power supplies** – cloud computing data centers have backup power supplies to run servers in case of power outages. In most cases, backup power is provided by diesel generators that can come online instantaneously in the event of a power failure and power the data center for as long as necessary until electricity is restored.
- **Redundant Internet connections** – cloud computing data centers have several Internet connections that run simultaneously. If one Internet provider fails or is performing poorly, they are able to use other providers that have different Internet backbone services.
- **Redundant hardware** – tier 4 data centers use multiple hard drives and other components, arranged in such a way that if one fails another can immediately and seamlessly take its place.
- **Fire and flood** – the data at most data centers is replicated in multiple locations. In the case of a fire, flood, or other disaster, your applications and data can be easily accessed by another computer in another location.
- **Theft** – data center servers are not easily accessible. Only authorized agents have access to them, and their identity is verified using biometric measures like fingerprints and retina scans. In addition, the entire data center is monitored by surveillance cameras at all times.

APPLICATION SECURITY

Application security covers the software side of the data center. It deals with online security issues like hackers and viruses. Application security measures include:

- **Firewalls** – firewalls act as an electronic barrier between the data center and the Internet. They limit the execution of files and access to data to ensure that hackers and other unauthorized parties cannot access data.
- **Antivirus detection software** – constantly updated, antivirus software detects and removes any viruses that penetrate the data center environment.
- **Data encryption software** – this software encrypts data as it travels between your organization and the data center.
- **Administrative controls** – data centers use administrative controls to govern access to applications and data. They limit access to certain functions and protect your files.

- **Security audits** – cloud computing providers conduct regular third-party intrusion detection audits. This means they actually hire professional hackers to try to hack into their applications and provide audit reports with their findings. These audit reports highlight any security holes in the applications and infrastructure, which can then be dealt with by data center technicians.

WHAT'S MY ROLE IN CLOUD COMPUTING SECURITY?

As we've seen above, most cloud computing providers take extraordinary measures to keep your data safe on their end.

But the fact is, the biggest risk to your data comes from inside your organization, from misrouted data and other simple mistakes to outright data theft by employees.

Cloud computing offers much better protection from internal data loss than other communication methods because it gives you centralized control over your data. It's much easier to establish and enforce policies for a cloud-based system than for the patchwork of email accounts, physical media, and thumb drives that usually results from on-site data storage. However, you are still responsible for establishing and implementing those policies effectively.

The tools you can use to manage access to data include:

- **Administration modules** – most applications have an administration module that allows a system administrator in your organization to grant user access rights and place restrictions on who can access which files and functions.
- **Organization usage policies** – usage policies are one of the most important tools you have for protecting your data. Can your employees access your systems in public locations where observers can view sensitive data? Can sensitive data be exported to unsecure media and distributed? Can sensitive data be emailed or transferred via unsecure methods?

Your cloud computing provider can work with you to establish good user policies. But ultimately, it's up to you to make sure they're communicated to employees and enforced.

WORKING WITH YOUR CLOUD PROVIDER

Trusting an outside company with something as important as your data can be a difficult adjustment for some organizations. But if you choose your hosting company carefully and approach implementation with the right knowledge and expectations, the process can be surprisingly painless.

It's a good idea to look at your relationship with your cloud computing provider as an ongoing partnership rather than a vendor-customer relationship. Considering them an extension of your work will open the lines of communication and help you build a relationship that's mutually rewarding.

The most important thing to remember when you're working with your cloud computing provider is that **you own your data**. The provider should manage the infrastructure and application availability, but they should not have access to your data without your permission.

Here's a quick guide to the ins and outs of managing data between you and your provider:

- **Your cloud computing provider may need to access your data.** They should have policies in place to ask for your permission to access your data when support is needed.
- **You should not assume that support personnel can access your files at will.** Remember, you have the right to deny support personnel access to your data.
- **Most cloud computing providers have data logs in place,** so there is a record of who has accessed your data and when that access took place.
- **It is important to read the privacy statements in your cloud computing provider contract agreements.** These statements will outline how they maintain privacy of your data and what measures can be taken if it is violated.
- **You should ensure that your provider will not use your data for marketing or promotional activities.** In such cases, you should have the ability to opt in to such marketing communications.
- **Remember, it's your data,** and you are ultimately responsible for the privacy of that data.

NOTE: Although we are highlighting these data privacy concerns in this white paper, these concerns are not isolated to cloud computing providers as they can be issues in protecting data within your own organization as well.

QUESTIONS AND ANSWERS

Not all cloud computing providers are created equal. The list of questions below should help you evaluate different providers as you look for the company that can best meet your needs.

How many years have you been providing cloud computing solutions? Look for a provider that has demonstrated years of experience in cloud computing solutions. Cloud computing has been around for more than 10 years, and the most experienced vendors have worked through all its complexities.

What class of data center do you use? Look for providers that offer tier 4 data centers. Tier 4 data centers offer built-in redundancies that are important for protecting sensitive data.

Do you have backup data centers? Is my data replicated at multiple data centers? Providers with backup data centers can ensure uninterrupted service in case of infrastructure failure. This will also demonstrate the level of investment the provider has dedicated to your cloud computing solution.

Have you ever had a security breach? When and how will you notify me if there is a security breach? Hopefully, your provider has never had a security breach. If they have, find out what they learned from it and how they plan to prevent it from happening again. Also, make sure they have procedures in place to notify you if a breach does happen.

What experience do you have with the legal industry and the public sector in particular? Attorneys have a duty to safeguard sensitive information, which makes many attorneys understandably wary about placing confidential data on a vendor's servers. Make sure that your cloud computing vendor is sensitive to the security needs of attorneys, especially those in the public sector. Learning how they've secured sensitive data for other government organizations will help you understand their level of experience with the legal profession and public sector.

What is your largest customer? The answer to this question can help you determine whether the size of your organization is a good fit with the resources the provider has to offer.

If I use your company to store my data, will it be accessible to anyone on the Internet? There are two types of cloud computing services. The first type is public cloud computing, which hosts public applications like Yahoo and Google. These types of services are publically accessible via the Internet. The other type is called private cloud computing. These applications are restricted between the cloud computing provider and their clients who subscribe to the service. Most business applications are private cloud computing applications.

How will I be able to access my data? You need to discuss the types of data access that your cloud computing provider offers. You should also discuss how you will receive your data should you choose to switch cloud computing providers and move your data to a new location.

Should I be concerned about the security of public wireless Internet connections, such as those at coffee shops? Each environment carries its own set of security risks, and public Internet connections are no exception. However, most cloud computing solutions use secure encrypted communications. These sophisticated encryption methods help ensure that even if someone does intercept your data, they will not be able to decipher it. To ensure that you are running an encrypted connection, simply look at the URL of the web address. It should say "HTTPS://" not "HTTP://".

What policies do you have in place to protect the privacy of my data? Make sure the provider's employees understand how to protect your data. Ensure that they have procedures in place to maintain their standards.

What types of security audits do you perform on your systems to protect me from hackers? Look for providers that contract with third party intrusion detection audits. This demonstrates an ongoing commitment to maintaining the highest level of security.

What happens to my performance if your client base grows rapidly? Is your system scalable? You should make sure your provider is monitoring the load on their servers and has a proactive plan in place to add servers if necessary.

How many clients do you have in your shared cloud computing environment? Most providers offer a shared infrastructure. Make sure they have a significant number of clients using their cloud computing solutions. This demonstrates experience, client satisfaction, and scalability.

Can I visit a data center to inspect the facilities? Many data centers provide scheduled tours of their facilities. These tours will highlight the data center's physical security capabilities and technology.

How can you help me optimize performance if my applications don't work well with your hosting? Cloud computing providers should have technical experts on staff that know how to optimize application performance over the Internet.

How do you monitor your system performance? Experienced cloud computing providers should have sophisticated tools for monitoring their servers and performance metrics. They should manage system availability and schedule system maintenance in a way that minimizes disruption.

How is your support team trained to protect the privacy of my data? What kind of support can I expect? The support team at any cloud computing provider should have strict procedures in place for protecting the privacy of your data, and they should be enforced consistently.

READY TO GET STARTED?

Choosing a cloud computing provider is a big decision. But a good provider should be more than happy to answer your questions and help you find the right solution. And once you do implement cloud computing, you're likely to find that it's one of the best and most cost-effective investments your organization has made.

If you'd like to talk with a Thomson Reuters representative about our cloud-based products, call us at **1.888.728.7677** or visit us at **legalsolutions.thomsonreuters.com/findYourRep**



THOMSON REUTERS™

© 2013 Thomson Reuters L-386243/7-13

EMERGING LEGAL TECHNOLOGIES AND WORKFLOW CHALLENGES FACING PUBLIC LAW OFFICES

WHITE PAPER



THOMSON REUTERS™

BACKGROUND

What started as a trend is now a fact: public and nonprofit law offices and departments face greater workload challenges in an environment of diminished resources. The question that persists is not only one of how to successfully meet the demands, but how to do so more efficiently. This is a pervasive concern that affects legal departments in the private sector as well.

In search of an answer, Thomson Reuters recently completed in-depth research with more than 500 public sector legal department leaders, attorneys, and staff. A survey explored their key tasks and how they complete those tasks today, and detailed conversations were conducted to get a richer understanding of their daily challenges. Thomson Reuters also interviewed experienced managers in legal support programs whose mission is to deliver the technology systems and tools and the practice support that lawyers depend upon to manage their matters and related work.

The results of the survey and interviews provide an in-depth look at enhancing productivity in public sector legal departments – identifying specific bottlenecks and opportunities to leverage technology to improve workflows.

Some public sector legal professionals describe their current system, pain points, and needs as follows:

- *"All ad hoc on my own"*
- *"There should be a way to share information securely through an online document repository"*
- *"We need user friendly programs and good documentation, easy to learn and easy to solve the problems"*
- *"There's a need for secure, remotely accessible document storage for documents that must be shared outside the office"*

INCREASING RESPONSIBILITIES WITH STAGNANT OR SHRINKING RESOURCES

Expectations for government and nonprofit legal departments are rising. The demands of a growing workload place new strains on departments struggling to control, if not reduce, costs in an era of fiscal restraint. They face more challenges than ever, with rising case complexity, document volume, and discovery rules. Investments in hardware or software upgrades that were postponed are reaching the critical point where delay is no longer an option as existing equipment and applications are inadequate to meet the practical needs of a 21st-century law department.

As a result, the current work processes environment in government legal departments has been described as "outdated," "inefficient," or "virtually total incompatibility."

The situation is not uncommon. Busy lawyers need help to make the tools they have today work better and to be assured that new and upgraded tools will integrate seamlessly. As importantly, lawyers and other legal professionals want user-friendly programs that are easy to learn, intuitive, and easily solve problems.

MANAGING MULTIPLE PLATFORMS ACROSS THE WORKFLOW

Making sense of the lack of a cohesive and collaborative work environment and how it can be addressed begins with identifying key factors that erode efficiency every day. Our conversations identified major obstacles legal departments encounter across their workflow, regardless of matter type. Additionally, they identified characteristics a successful technology solution should include. As one legal professional in the public sector stated, there is "too much time wasted entering things into several different places." Collaboration, accessibility and security are key concerns shared by many as well. In fact, one lawyer simply stated "we need systems that allow us to share information within the office and with our clients in a secure, remotely accessible manner."

CRITICAL TASKS AND TECHNOLOGY ADOPTION

The research identified a growing desire for applying technology solutions to address the lack of consistency, standards and procedures, improve efficiency, increase productivity, reduce costs, improve outcomes, manage risk, and more effectively demonstrate the benefits of the investment.

In addition to the overarching challenges detailed above, the survey identified critical task categories. We defined "critical" as: 1) core to the law department's mission and role (as judged by respondents), and 2) having highly negative impact if errors are made (as judged by respondents). We focused on tasks that are widespread and performed by more than half of surveyed law departments.

The survey found that some critical tasks are currently being addressed through use of vendor-provided automated software tools. The majority of law departments in the public sector (67%) use vendor tools, such as Westlaw®, for legal research. Matter and case management tools, such as Case Notebook™, have been adopted by 35 percent of respondents.

However, the research identified four top tasks (outside of pure legal research) that are widespread among government legal departments. These other critical tasks included the following: legal drafting (73%); managing document review and discovery (62%); collaborating with team members and client agencies (58%); and managing legal/litigation holds (61%).

AN EXPANDED VIEW OF ENTERPRISE LEGAL MANAGEMENT

Using stand-alone solutions for any one of these critical tasks is beneficial, but falls short of solving all of the day-to-day challenges presented above. Rather than applying discrete solutions to each problem, or step in legal professionals' workflow, an integrated solution would address many of those challenges described earlier in this paper.

Today, the term Enterprise Legal Management (ELM) is being used to describe systems that tackle multiple legal department operations. Though still an evolving term, solutions included in the definition of ELM include: matter management, document management, and process management. We believe that this limited definition excludes many of the tools that public lawyers and staff use on a daily basis.

Based on our findings, we believe that the full benefits currently ascribed to ELM cannot be achieved unless such a system includes tools for several, if not all, of the top tasks listed above. Without that integration, law offices and legal departments will still have many of the nagging problems of multiple tools – such as duplicate data entry, ad hoc processes, multiple storage locations, and missed collaboration and sharing opportunities. They will still contend with the possibility of inconsistent positions on legal issues, security concerns, and redundant costs. They will still grapple with discovery compliance and litigation holds.

A more comprehensive definition of ELM, and a system that delivers it, would be transformative for law department management, lawyers, and staff. Managing lawyers and administrative staff get a comprehensive view of the department's activities. Lawyers and staff are made more effective and efficient by applying automated solutions within the matter. Data is surfaced in-context for decision making.

Collaboration with other counsel and client agencies goes beyond status updates and shared drives to full engagement in real time using the device available to each party, whether desktop, laptop, tablet, or devices not yet imagined. A centralized, integrated system has the potential to allow law offices and legal departments to gain more control over their workload and better meet the legal needs of their organizations, agency clients, and stakeholders.

THOMSON REUTERS CONCOURSE™

Concourse helps you organize all matter-related information in one intuitive place, share documents, assign tasks, track deadlines, create legal holds, and collaborate more efficiently with colleagues. Concourse integrates seamlessly with WestlawNext® and Microsoft® Outlook®, and also allows you to access matter-related information straight from your mobile devices.

Learn more at **about.concourse.thomsonreuters.com/gov**.



PRESERVATION AND LEGAL HOLDS IN THE PUBLIC SECTOR

BY JAY E. GRENIG, PROFESSOR OF LAW
MARQUETTE UNIVERSITY LAW SCHOOL

INTRODUCTION

Government agencies (whether at the city, county, state, or federal level) have traditionally been the repositories of massive amounts of information. The rapid increase in recent years of electronically stored information and the variety of systems or devices for creating and storing such information has dramatically increased the amount of stored information. Additionally, electronically stored information frequently can be found in a wide range of locations and sources, including desktop computers, laptop computers, network hard drives, removable media, servers, backup tapes or other storage media, personal digital assistants, cellular telephones, Internet websites, paging devices, GPS navigation systems, photocopies, audio tapes, videotapes, and voice mail.

Unlike paper documents, electronically stored information has dynamic content likely to change over time, even without human intervention. Workflow systems may automatically update files and transfer electronically stored information from one location to another. Web pages are constantly updated with information fed from other applications. Email systems may reorganize and remove electronically stored information. Merely accessing or moving electronically stored information can modify it.

Organizations in both the public and private sector are increasingly concerned about the necessity of preserving this quantity of electronically stored information. A government agency's failure to preserve information may have serious consequences. This paper will explore the issues, and pitfalls, regarding preservation of electronically stored information facing government agencies today, as well as processes and best practices in dealing with the duty to preserve.

The duty to preserve involves taking reasonable steps to protect information for potential audits, investigations, administrative proceedings, or anticipated litigation. In addition, government agencies may be required to preserve certain information by open records laws or other statutory mandates. *See, e.g., Chambers v. U.S. Dept. of Interior*, 588 F.3d 998 (2009). The duty to preserve may arise under statutes, administrative rules, or a "legal hold."

A "legal hold" is a communication suspending the normal disposition or processing of information. It is sometimes called a "litigation hold" or a "preservation order." An opposing party may send a legal hold notifying the other party of the need to preserve electronically stored information and the scope of preservation. A legal hold is also sent to employees and clients notifying them of their duty to preserve specified electronically stored information.

Due to the qualities of electronically stored information, it is important to take steps to preserve the integrity of the contents of electronically stored information. Depending on the nature of the information to be preserved and circumstances of the requirement, this may include preserving information about the formatting of the document, its metadata,[1] and its revision history. Preservation can be accomplished in various ways ranging from evidentiary imaging prepared by a forensic professional to simply taking custody of a laptop or backup tapes.

[1] The term "metadata" means other data providing information about a certain item's content, who the author is, when the document was written, and a summary of the document.

If a government agency fails to preserve electronically stored information, the agency may be sanctioned for "spoliation." According to *The Sedona Conference® Glossary: E-Discovery & Digital Information Management* (third edition), "spoliation" is "the destruction of records or properties, such as metadata, that may be relevant to ongoing or anticipated litigation, government investigation or audit." Sanctions for spoliation include reprimands, monetary penalties, dismissal, default judgment, and negative inference jury instructions.

TRIGGERING THE DUTY TO PRESERVE

In the context of civil litigation, the duty to preserve electronically stored information and paper documents is triggered when litigation is "reasonably anticipated." *See, e.g., AAB Jt. Venture v. United States*, 75 Fed. Cl. 432 (2007) (government's duty to preserve electronic evidence with respect to contractor's differing site conditions claim arose when contracted requested equitable adjustment relating to subsequent litigation were filed); *Disability Rights Council of Greater Washington v. Washington Metro. Transit Auth.*, 2007 WL 1585452 (D.D.C. 2007) (although the complaint was filed on March 25, 2004, WMATA did nothing to stop its email system from obliterating all emails after 60 days until June of 2006); *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003). The duty is imposed on both plaintiffs and defendants. The duty to preserve attaches to a plaintiff upon contemplation of litigation. *See, e.g., Micron Technology, Inc. v. Rambus*, 255 F.R.D. 135 (D. Del. 2009). A defendant's duty to preserve begins when litigation is pending or reasonably foreseeable.

Government agencies and their lawyers must act quickly once they receive notice of litigation or reasonably anticipate litigation. Now that 99% of information is created and stored electronically and users can delete information easily, the identification of custodians, sources of electronically stored information and the implementation of a preservation plan must happen quickly.

While technology has created some of the problems associated with discovery of electronically stored information, technology can also be used to ease the burden. For example, Thomson Reuters Concourse™ helps draft and distribute legal hold notices to all custodians, upload files for custodians to review, and automate reminders for non-responders.

ASSESSING SCOPE OF DUTY TO PRESERVE

Because it is impractical to put an entire government agency on hold every time litigation is anticipated, agencies should work to create a narrowly tailored plan preserving the information required for the litigation while allowing the agency to continue to function normally. Negotiating narrowly targeted preservation allows the agency to understand the scope of its duty to preserve and prevents the other side from conducting a fishing expedition. Counsel who cannot agree after attempting to negotiate the scope of preservation should seek the court's assistance or request a special master. In-depth involvement of internal and external information technology staff is almost always necessary to accomplish this goal.

Although an agency is not under a duty to keep or retain every document in its possession, an agency must preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery or is the subject of a pending discovery request.

An agency must retain all relevant documents (but not multiple, identical copies) in existence at the time the duty to preserve attaches, and any relevant documents created afterwards. The duty to preserve extends to those agency employees likely to have relevant information (the "key players" in the litigation). Whether the agency is required to preserve unsearched sources of potentially responsive information it believes are not reasonably accessible depends on the circumstances of each case.

IDENTIFYING ELECTRONICALLY STORED INFORMATION TO PRESERVE

Identification involves determining the scope, breadth, and depth of electronically stored information that may be sought during discovery. The identification process should take into consideration any claims and defenses, preservation demands, disclosure requirements, and discovery demands. In identifying electronically stored information that might be pursued during discovery, it is helpful to start from a larger pool of potentially discoverable electronically stored information and then assess how much should be preserved and collected.

For government agencies, identifying what electronically stored information to preserve can be an expensive and time-consuming burden. The most effective way to preserve information for litigation is to identify the types of information implicated in the suit as well as the custodians. A government agency should conduct interviews and surveys of those custodians as soon as possible. It is important for counsel to negotiate the scope of the information to be produced with opposing counsel.

Government agencies should not rely on their own understanding of what constitutes electronically stored information or how it should be preserved. They should ask their lawyers for assistance. Government agencies may also retain outside counsel knowledgeable and experienced in e-discovery to provide appropriate guidance. Government lawyers and experienced e-discovery counsel are in a position to determine:

- What systems are included in an organization's information technology infrastructure.
- Where the most relevant types of electronically stored information may be stored.
- What metadata exist and how metadata ought to be preserved.
- What backup or data storage sequences should be suspended.
- What steps should be taken to image hard drives.
- What steps should be taken to separate business email from personal email or otherwise protect employee privacy or trade secrets.
- What must be done to distinguish between unique and duplicate electronically stored information.
- What steps should be taken to preserve Web pages or intranet systems.
- The most cost-efficient and reasonable process for handling electronically stored information.
- How to negotiate the scope of preservation and form of production.

PRESERVING ELECTRONICALLY STORED INFORMATION

Typically, preservation focuses on preserving electronic media – hard drives, floppy disks, and backup tapes, for example – rather than particular files, folders, or other forms of data. Preserving media, as opposed to preserving just the electronically stored information that appears responsive or interesting initially, preserves not only the potentially responsive data, but also files and other data that could become important as discovery progresses. Preserving media also preserves other information, such as metadata or deleted material, that could be used later to corroborate or authenticate the produced electronically stored information.

One of the most common preservation mistakes is failing to cease document destruction procedures upon notice of suit or when the likelihood of suit or investigation becomes reasonably apparent. The destruction of electronically stored information during the routine implementation of a document retention policy in the usual course of operation is normally acceptable. Once a government agency reasonably anticipates litigation, however, it must suspend its routine document destruction policy and put in place a legal hold (also known as litigation hold).

A government agency must evaluate the extent to which retention policies must be suspended because of the duty to preserve. Although systematic suspension of routine document destruction is one way to protect an agency, it usually is not the most efficient or cost-effective way to manage preservation. Normal day-to-day operations among government agencies, departments, and employees, as well as the information technology departments that support them, have the potential to destroy or alter critical sources of digital information. Routine operations such as archive rotation, document deletion schedules, or simple computer use will alter electronically stored information.

Agencies must give special consideration to archived media, such as backup systems. Frequently, system administrators will only maintain a limited quantity of backup media, and then reuse them on a scheduled cycle – known as tape rotation. If backup systems are implicated – meaning that the information is not available from another active source – an agency should ensure that all relevant backup media are preserved by someone who can later establish a chain of custody for authentication purposes.

Not all electronically stored information will be on an agency's systems. Responsive electronically stored information may be in the possession of contractors, agents, vendors, clients, lawyers, accountants, consultants, experts, and former employees. Nonparties over whom the agency has control or influence must be factored into the preservation process.

Preservation does not mean that an agency must later agree to produce evidence. By preserving electronically stored information, an agency is only assuring that the electronically stored information will be available if the information is later determined to be relevant or discoverable.

INFORMING EMPLOYEES OF DUTY TO PRESERVE

Agency employees are notified of their duty to preserve by means of a written legal hold notice. The goal of a legal hold is to prevent any alteration or destruction of electronically stored information. A legal hold notice is used to clarify and document a party's preservation plan and efforts. It is advisable to use a written legal hold to demonstrate the efforts undertaken in identifying and preserving sources of information potentially relevant to the case at hand. When used in connection with an overall discovery plan, a legal hold notification (whether written, via email, or through a vendor-provided technology) provides counsel with a framework to negotiate scope and proportionality issues at the discovery conference.

A legal hold places key custodians of information on notice of their obligation to preserve. To properly accomplish this goal, the communication must be clear, provide enough contextual information to describe the issue, explain the process, explain the consequences for not complying, and describe how the preservation will be effectuated. While a legal hold notice may follow a common form and style, it should not simply be a recitation of boilerplate language.

The legal hold notice is typically distributed to any custodian of data potentially relevant to the litigation. This includes named parties, their managers, and assistants. The information technology administrators will also be included because they control or manage network information. These information technology personnel often play a critical role in assessing and ultimately preserving information sources relevant to the case. Government lawyers should take care to include and send the legal hold notice (or a similar communication) to any third-party services providers that may maintain electronically stored information on behalf of the agency. This may include email providers, communication providers or any other outsourced service provider.

The following subjects are typically covered by a legal hold notification:

- **Description of the litigation.** It is necessary to provide enough detail so the recipient can properly assess what information is subject to the hold.
- **Identification of key custodians.** Depending on who receives the legal hold, it may contain a list of custodians subject to the hold. The list should be thoroughly discussed with counsel and client to determine the list of individuals that are properly subject to the hold.
- **Identification of information subject to the hold.** Counsel should review a data map or otherwise identify sources of potentially responsive information with the client. These sources should be clearly identified in the legal hold notice. If communications are implicated, the notice should identify and include methods of communication such as text messaging, Twitter®, blogs, Facebook®, and other social media.
- **Guidance on how the hold will be effectuated.** The notice should clearly tell employees how and when the information in their possession will be preserved. If the preservation is not immediate, the notice should explain to the employee what to do before the preservation (e.g., do not delete email, do not modify files).
- **Describe consequence for failure to comply.** The notice must communicate to the employees the consequences for failing to comply with the legal hold.
- **Provide contact information.** The notice must provide contact information in case employees have questions.

If a key custodian is also a named party in the litigation, consideration should be given to the need to effectuate some form of preservation before distributing the legal hold. For example, if a manager has been named in a sexual harassment suit, the distribution of the legal hold may provide warning and incentive for the manager to destroy information within the manager's custody and control. In such a situation, counsel would be better advised to preserve the manager's data before or contemporaneously with the delivery of the legal hold letter.

LEGAL HOLD PROTOCOL

Every agency and department should adopt a formal, written records and information management program, including a legal hold protocol. The legal hold protocol should be a reasonable, repeatable process that is routinely followed by the organization each time it receives notice of, or reasonably anticipates, litigation.

New technologies and products can assist government organizations with their legal hold processes – making them more automated, efficient and defensible in court. Features such as email "read receipts" and logging, automatic custodian acknowledgement reminders, and response tracking not only help with some of the manual, time-consuming processes, but also provide "proof" of due diligence when effectuating a hold.

A legal hold protocol focuses on preserving electronically stored information once litigation is foreseeable. The success of a preservation plan depends to a very large degree on counsel's intimate knowledge of the administrative controls and architecture of the client's computer system. For attorneys who do not regularly practice in the e-discovery arena, such knowledge can only be acquired by retaining experienced counsel with knowledge of the technical issues. This is especially important when it comes to devising workable preservation plans.

Organizations making reasonable efforts to put a legal hold in place and to preserve information relevant to the dispute will fare better in front of a judge than those that do nothing. Destruction of potentially relevant information must not be done in bad faith. Bad faith may include suddenly following the destruction schedule to limit damaging evidence available to potential litigation adversaries.[1]

LITIGATION HOLD LETTERS TO OPPOSING PARTIES AND PRESERVATION ORDERS

In appropriate cases, a party may seek a preservation order from the court ordering a producing party to preserve electronically stored information. *See Valdez v. Town of Brookhaven*, 20070 WL 1988792 (E.D. N.Y. 2007). Because preservation orders are burdensome and expensive, in the absence of a clear need preservation orders should not be entered without a particularized showing of a need. *See Pueblo of Laguna v. United States*, 60 Fed. Cl. 133 (2004) (proponent of order preserving evidence must show the particular steps to be adopted will be effective, but not overbroad).

Another important tool is a preservation letter sent to an opposing party. The letter places the other party on notice with respect to its duties to avoid spoliation. It also serves as an excellent basis for seeking sanctions, if it is later discovered that spoliation did in fact occur. Plaintiffs, defendants, and third parties from whom discovery is sought should use the preservation letter to initiate the conversation regarding the scope of the duty to preserve.

A preservation letter should be sent to the other party or the other party's attorney at the earliest possible moment, describing the electronically stored information to be preserved. It should request a meeting to construct a mutually acceptable plan for the production of electronically stored information. A preservation letter should be sent before, or at the same time as, the commencement of litigation and well before any voluntary disclosures by a party under Fed. R. Civ. P. 26 and before any discovery has occurred.[1]

A preservation letter is not a discovery request; it is simply a request that the other party preserve the party's electronically stored information so that it is not deleted or altered through intentional misconduct or the normal processes associated with the deletion of computer files due to the ongoing business of a party. A party can disregard the request to preserve, but once the request has formally been made and evidence disappears, a preservation letter may place the discovering party in a superior position to seek sanctions or other relief.

The content of a preservation letter should be carefully thought through by counsel and be grounded in a firm understanding of the types of electronically stored information the other side likely has, as well as what types and forms of information will be relevant to the dispute at issue. The letter should be narrowly tailored to reflect the scope of the dispute and avoid overly broad and burdensome requests for organizations to cease purging any information, but specifically limit it to relevant information.

Counsel drafting the letter should have a general understanding of the sources of electronically stored information the party may have available. Counsel should be prepared to request a Fed. R. Civ. P. 30(b)(6) deposition of the individuals with the most knowledge of the types of electronically stored information available in the organization.

At a minimum, a letter should begin with a general statement that the discovering party expects the party to preserve electronically stored information evidence that may be relevant to the issues in a case, or may lead to the discovery of such evidence. The preservation letter should include a request that the other party suspend its regular document retention policy for relevant information pending discovery and identify all possible locations where such evidence might conceivably reside.

The letter should inform the opposing party that a mere file backup of the hard drive is not adequate preservation. The party must be instructed to image hard drives in bitstream copies, where all areas, used and unused, of the hard drive are copied. If a file is deleted before a backup is made, the deleted file will not be copied unless it is a bitstream copy. The letter should also request that deleted files that are reasonably recoverable be immediately undeleted.

Writing a preservation letter is not an idle gesture. Although a party has the duty to protect and preserve evidence once it is on notice that it must do so, a preservation letter must be specific with respect to the matter in dispute for a court to find that it put a party on notice for preserving specific types of information. Courts have held that a party may be under a duty to prevent spoliation even if litigation is only reasonably anticipated.[1] Serious sanctions may be imposed for failure to preserve information once a party reasonably anticipates or is on notice of litigation.

SANCTIONS FOR FAILURE TO PRESERVE

Spoliation is the destruction, significant alteration, or failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation. *See Sampson v. City of Cambridge*, 251 F.R.D. 172 (D. Md. 2008). Spoliation can be inadvertent or intentional. It can be the product of absolute good faith or the exercise of consummate care.

A party seeking sanctions for spoliation must establish that:

- the party having control over the evidence had an obligation to preserve it at the time it was destroyed,
- the records were destroyed with a culpable state of mind, and
- the destroyed 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.

See, e.g., Passlogix, Inc. v. 2FA Tech., LLC, 708 F. Supp. 2d 378 (S.D. N.Y. 2010); *Barsoum v. NYC Housing Auth.*, 202 F.R.D. 396 (S.D. N.Y. 2001).

If a court determines a person or organization disposed of or failed to preserve discoverable evidence including electronically stored information in the face of reasonably foreseeable litigation, the court has considerable discretion in deciding whether sanctions should be imposed for the spoliation. *See, e.g., Buckley v. Mukasey*, 538 F.3d 306 (4th Cir. 2008); *Fujitsu Ltd. v. Federal Exp. Corp.*, 247 F.3d 423 (2d Cir. 2001). Determining whether sanctions are warranted and, if so, what the sanctions should be requires a court to consider both the spoliating party's culpability and the level of prejudice to the party seeking discovery. *See, e.g., Buckley v. Mukasey*, 538 F.3d 306 (4th Cir. 2008); *Rimkus Consulting Group, Inc. v. Cammarata*, 688 F. Supp. 2d 598 (S.D. Tex. 2010). Whether sanctions are appropriate and what level of sanction should be imposed turn on three key factors:

- the degree of fault of the party who altered or destroyed the evidence;
- the degree of prejudice suffered by the opposing party; and
- whether there is a lesser sanction that will avoid substantial unfairness to the producing party, and, where the producing party is seriously at fault, will serve to deter such conduct in the future.

See, e.g., Micron Tech., Inc. v. Rambus, Inc., 645 F.3d 1311 (Fed. Cir. 2011).

A sliding scale of sanctions may be imposed depending on the degree of control the alleged spoliator had over the evidence and the spoliator's subjective intentions. The severity of a sanction must be proportionate to the culpability involved and the resultant prejudice. *See Webb v. District of Columbia*, 146 F.3d 964 (D.C. Cir. 1998). Sanctions for spoliation include:

- Criminal penalties
- Unfavorable evidentiary presumptions
- Discovery sanctions
- Dismissal of lawsuit
- Adverse inference jury instruction
- Monetary penalties including reimbursement of attorney fees
- Striking an answer
- Barring the presentation of evidence relating to the destroyed evidence
- Default judgment

CONCLUSION

With proper planning, it is possible to reduce the costs and risk relating to discovery of electronically stored information. Government agencies should work with legal counsel and information technology staff to develop a plan for how to preserve and produce documents quickly and efficiently. Government agencies must understand which e-discovery functions can be performed with technology and which functions require human involvement. Finally, an agency must put a person knowledgeable in the law and technology in charge of e-discovery efforts. Technology such as Thomson Reuters Legal Hold can automate the legal hold process.

ABOUT THE AUTHOR

Professor Jay E. Grenig is a Professor of Law at Marquette University Law School. He has also taught at the University of Southern California Graduate School of Public Administration and the Cornell University School of Industrial and Labor Relations. Professor Grenig is the author or co-author of numerous books and articles including *Fundamentals of Government Contracting, Electronic Discovery and Records and Information Management Guide,* and *Alternative Dispute Resolution*. Professor Grenig is a member of the National Academy of Arbitrators, the American Law Institute, and the Order of the Coif. He is also a fellow of the College of Labor and Employment Lawyers.

CONCOURSE LEGAL HOLD

Concourse Legal Hold assists with implementing and automating the legal hold process to reduce risk and maintain compliance. It provides a repeatable, defensible method for tracking and reporting on the delivery of hold notifications and custodians' acknowledgements – essential with courts increasing penalties for spoliation claims.

Learn more at **about.concourse.thomsonreuters.com/gov**

MATTER ROOM

Connecting everything about a matter in one place.

THOMSON REUTERS CONCOURSE

Thomson Reuters Concourse™ is a matter-based suite of products that makes managing a legal department easier – and your attorneys more productive. Concourse seamlessly integrates with the tools you use everyday like WestlawNext®, Microsoft® Outlook®, and Microsoft Windows®, ensuring everything you need is exactly where you need it. With Thomson Reuters Concourse, you can organize your department's legal activities, save time and money, and expand your capabilities.

In a secure, private cloud environment that is accessible wherever you have Web access, Concourse Matter Room enables you to easily organize your matters, upload emails and documents, collaborate with internal teams and external partners, review and annotate work product, keep track of important tasks, and analyze time spent on matters. It connects you to what matters: people, documents, research, emails, and more.

Matter-based collaboration space

- Allows you, your team, and other partners both inside and outside your agency to access all your matter-related activity in a secure permissions-based environment
- Functions as a centralized repository to upload documents, emails, and images, and share them with those you designate
- Enables organization of emails, documents, and contacts related to a matter in one place so all participants can access them from anywhere

Powerful searching across matters

- Search precisely across matter documents and communications
- Leverage the revolutionary Thomson Reuters search technology behind WestlawNext to find what you are looking for
- Save time by allowing you and others working on a matter to reuse past work product and save the costs of reinventing the wheel
- Access related materials via automatically generated live citation linking within your documents
- Access KeyCite® citations within documents to ensure you are citing good law

Integration with everyday tools

- Connects the tools you use every day, such as Microsoft Outlook and WestlawNext
- Virtual folders make it easy to put matter-related material in one place to streamline collaboration

Time Tracking created specifically for government

- A streamlined and easy-to-use Time Tracking tool addresses the need to analyze time for resourcing and department management
- Time Tracking allows users to easily track time by matter, activity, and Custom Matter Fields
- Associate time with preloaded task categories and/or create custom categories
- Identify tasks, client agencies, or matters that are consuming resources. Allows you to see time at matter, individual, or department level
- Information recording in the Time Tracking tool can be exported to a .csv file for analysis

Secure, mobile access from an iPad® or other tablet device

- All interactions are in Hypertext Transfer Protocol Secure (HTTPS) sessions, with the same encryption and transport standard used by banks, brokers, and businesses
- Matter Room automatically encrypts documents, emails, and notes and stores them in one of the world's largest data centers – Class IV and IBM®-certified
- Matter Room security is assured through strict authentication and permissions that you control
- Cloud-based environment reduces the need for advanced hardware, software, licenses, and physical space to store data
- Access everything related to your matter from anywhere you have Internet access

Some exclusions apply. Additionally, certain content may be accessible only on WestlawNext. Content subject to change. Contact your representative for plan details.

iPad is a trademark of Apple, Inc., registered in the U.S. and other countries.

Visit thomsonreuters.com/concourse

To order or for more information, contact your representative at **1-800-344-5008**.

THOMSON REUTERS™

© 2013 Thomson Reuters L-380125/5-13

IMPLEMENTING AND AUTOMATING THE LEGAL HOLD PROCESS

Concourse Legal Hold provides a repeatable, automated, and defensible method for tracking and reporting on the delivery of hold notifications and the corresponding custodian acknowledgments. It provides an easy-to-use interface for both government legal departments and legal hold custodians, and integrates with other Concourse solutions.

THOMSON REUTERS CONCOURSE

Thomson Reuters Concourse is a matter-based suite of products that makes managing a legal department easier – and your attorneys more productive. Concourse seamlessly integrates with the tools you use every day like WestlawNext®, Microsoft® Outlook® and Microsoft Windows®, ensuring everything you need is exactly where you need it. With Thomson Reuters Concourse, you can organize your department's legal activities, save time and money, and expand your capabilities.

Systematic Process for Defensible Legal Holds

Concourse Legal Hold:

- Is essential at a time when courts are increasing penalties for spoliation claims
- Helps you reduce risk and maintain compliance
- Is superior to using email and spreadsheets
- Offers proven processes to initiate, manage, and track your organization's holds

Create New Holds

- When your organization has been sued or anticipates litigation, Concourse Legal Hold helps you easily draft and distribute a notice to all legal hold custodians
- Upload files for your custodians to review as well as create interviews to gain greater insight into the information they may possess
- Automate reminders for nonresponders
- Quickly determine the progress of any given hold

Collect Response Data

- Record custodians' acknowledgements and questions
- Send automated confirmations and reminders to document your organization's compliance

Track and Report

- View status of each hold on the Concourse Legal Hold homepage
- Track full details on legal hold-specific dashboards, including audit trails and released holds

Preserve Notifications and Responses

- After a matter resolves, Concourse Legal Hold provides secure storage of notices and custodian data
- Offers a documented trail of responses and nonresponses

Avoid Reinventing the Wheel

- Save notices and interviews as exemplars for future use
- Avoid starting new legal holds from scratch, saving you time and money

Control Permission Level

- Provides role-based access controls
- Easily select each user's permission

Learn more at
thomsonreuters com/concourse

THOMSON REUTERS™

© 2013 Thomson Reuters L-380284/2-13