

Legal Obligations Create Burden and Risk in IT Environment

by Deidre Paknad, President & CEO, PSS Systems
CGOC Publication June 2008



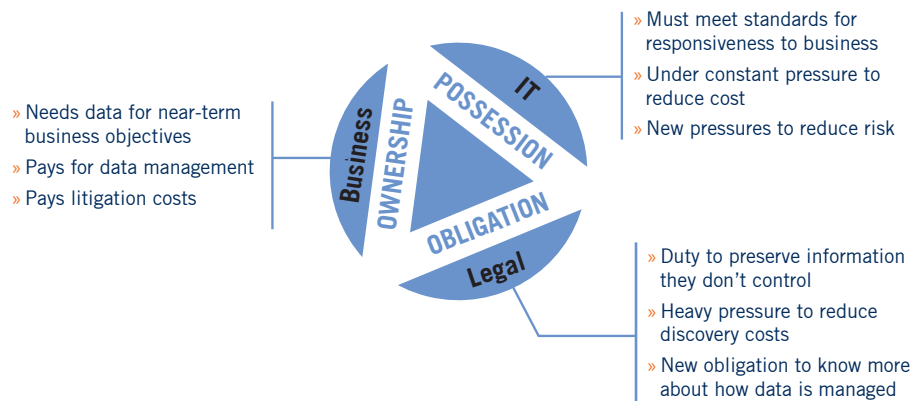
Background

Global companies face a myriad of laws that dictate how they handle information, specifically how long they must retain information, when they must preserve it as evidence, what uses are permissible while in their possession, and how and under what conditions it may be transported. Companies staff large legal departments to review, monitor and analyze such laws in the countries in which they operate; the legal department typically has a set of procedures it follows within its own organization to monitor and ensure appropriate compliance. Global companies must comply with well over 10,000 disparate legal retention, preservation, disposal and privacy duties. Unfortunately, while the legal staff has legal and professional obligations under the law for a broad array of information, they do not have custody or control of that information – this is the domain of corporate information technology management (IT) organizations.

The IT organization within companies manages literally thousands of systems and moves terabytes, if not petabytes, of information each year. The increasing rate of information flow combined with the increasing volume of information make it exceptionally challenging to move the data at the speed of business while also ensuring compliance with the many thousands of laws that dictate or constrain data management. Interpretation of law is the domain of lawyers and the corporate legal department, while transmission and management of data is the domain of IT management.

Ironically, most lawyers today use emails to send a single, narrow instruction from one lawyer to one IT person at a time; the many thousands of emails flying from legal to IT over the course of a month or a business quarter have significant risk and shortcomings:

- » Management transparency doesn't exist – only the individuals who sent and receive each email are aware of the legal instruction and proper response requirements
- » It is very difficult to monitor response or completion of any one legal instruction, much less monitor across legal instructions for compliance
- » Determining overlapping compliance obligations much less conflicting obligations is nearly impossible
- » IT staff are obliged to file and manage many dozens if not hundreds of individual emails from various attorneys to track their assigned tasks
- » When IT employees change roles or leave the company, it is difficult to transition their tasks to other staff, legal may be unaware of the change in personnel and legal duties may be forgotten in the process
- » Because legal tasks are not the primary day to day job duty of IT staff, a single email – even one with very important duties – may get lost in the onslaught of other, more routine activities



There are many significant fines, sanctions, judicial reprimands, and public relations disasters that epitomize the challenges and risks in synchronizing legal and IT domains and activities.

Another area of significant dysfunction is that attorneys and policy makers tend to think about different objects and elements than IT staff. Lawyers think about lawsuits and cases; records compliance staff think in terms of classification schemas and citations of law. IT staff, on the other hand, tend to think in terms of the specific systems they manage. Moreover, such systems may often contain data subject to multiple lawsuits and laws (citations). When legal and compliance instructions aren't readily understood by those who must follow or enforce them, error and risk are introduced.

Address these Challenges Systematically

In order to manage legal obligations over data with greater precision, global companies should implement a system which will link legal policy issuers and their context (laws, lawsuits) with IT staff who must implement such instructions in their context (systems and data types).

Companies should adopt a solution that is focused on helping legal and records management teams manage their workflows, helping them define the legal obligations and communicate them. By using a single legal governance system, IT staff more readily can understand those obligations and more efficiently address them.

IT Governance Hub

IT and legal teams require a single platform to ensure that data is managed in concert with company policy and country law. Global companies can benefit and more effectively manage the complexities by having a **web-based portal view of legal policies and instructions (retention, disposal, preservation of evidence, restrictions on uses, handling, or transport) for IT personnel which:**

- » Organizes and presents information in an IT context – organized by due date of the instruction or task, by system and data area the instruction applies to, by physical and business location in which the data is resident
- » Allows IT teams to manage large volumes of legal instructions across team members and across many applicable systems, including sharing responsibilities, delegating or distributing tasks among team members, viewing total current and past workloads for the team or by system area
- » Ensures tasks are completed on schedule by providing individual and team due date tracking, task aging, and alerts and reminders for near and past due legal policy tasks for IT staff and for the legal issuer
- » Ensures overlapping duties are visible so that the completion of one does not inadvertently suggest the completion of another duty (such as closure of one overlapping legal hold where several may apply which could lead to spoliation of evidence)

- » Enables conflicting duties to be resolved more easily by providing transparency to such conflicts, providing systematic feedback loops to the policy issuer, enabling online publication of conflict policies, and allowing policy issuers to determine and detect such conflicts before issuing confusing or conflicting instructions

The essential capability to understand and manage relationships of systems to:

- » Jurisdictions (countries, districts)
- » Lines of business (laws issued by various governing agencies)
- » Company departments and organizations (the business staff whose data resides in a given system)
- » Functional or business process classification schema (the type and context of the data in the system)
- » Make such relationships visible to both the appropriate legal policy issuers and the appropriate IT recipients

The ability to **limit the visibility of systems and legal policy instructions by a variety of criteria** for convenience and for compliance reasons – so IT staff see neither useless information nor restricted information, including limiting views and access by:

- » Geographic location of the system
- » Hierarchical level of the IT staff member
- » Line of business affiliation of the system
- » Type of system
- » Type of data managed within the system

Catalog and manage disparate systems to enable compliance with legal obligations, including the ability to:

- » Establish a taxonomy for systems by their type, kind, location, structure or other attribute to enable efficient organization of hundreds or thousands of systems
- » Define systems by key attributes relevant to legal obligations and compliance requirements including:

- ✓ accessibility of information within a system for US discovery rules
- ✓ accessibility of information within a system for US privacy rules or EU data protection rules
- ✓ format and structure of data in the system for US litigation requirements
- ✓ capacity of a system to secure personally identifiable information (PII) to country standards, confidential information
- ✓ capacity of the system to preserve data in the system that may constitute potential evidence, including its ability to inherently preserve, preserve with intervention by IT staff, or its inability to preserve
- ✓ stewardship of the system and its data, including those staff who have responsibility for preservation tasks, those who have responsibility for collecting evidence for legal matters, those who have responsibility for enforcing processing or access restrictions on the data
- ✓ related, successor and predecessor systems where data may or did exist and where legal obligations would therefore extend
- ✓ physical location of the system; physical location of the data originator which are essential for applying policies in compliance with governing laws in by jurisdiction
- ✓ the time frame in which the system contains active data, the date it was retired, and how data within the system was transferred or disposed upon system retirement

Create templates for system types that establish baseline attributes and characteristics, including those elements above, and enables these templates to be used to accelerate the cataloging and definition of similar systems

- » Enable IT staff to define systems, search through them by any combination of attributes, and update the definition and status of such systems through a convenient user interface, through online questionnaires accessed via emails, and other means

How is data deleted from the system?

Data cannot be deleted from the system	➔	Inherent ability to preserve in place	➔	Notice to Administrator	L1
Requires overt action by administrator to delete	➔	Inherent ability to preserve in place	➔	Notice to Administrator	L2
Can be deleted by users at their discretion	➔	Preventing user deletion necessary	➔	Can deletion be prevented systematically	

Can deletion be prevented?

System can be set to prevent deletion of data automatically	➔	Inherent ability to preserve in place	➔	Notice to administrator with confirmation of system settings, reminders	L1
System cannot be set to prevent deletion; normal use does not involve data deletion	➔	Inherent ability to preserve in place	➔	Notice to administrators and all users with confirmation of compliance; frequent reminders	L2
System cannot be set to prevent deletion; normal use may involve data deletion	➔	Preventing user deletion necessary	➔	Collect to preserve or notice to administrator and all users with confirmation of compliance; frequent reminders	L3

The ability to **detect compliance and non-compliance patterns** based on the attributes previously described and retention, disposition, preservation, processing, transport, and discovery policies and instructions through monitoring and business intelligence reporting. These may include:

- » Detecting where systems without the capacity to properly manage PII contain personal data in a jurisdiction where specific requirements for handling personal data exist
- » Detecting conflicts of jurisdiction law and obligations by analyzing the source of data (line of business and/or functional or process classification schema and its geographic location) and the location of the system containing the data (its geographic location), the legal duties that arise from the two jurisdictions, and the legal policies instituted for the system to determine if such policies are compliant
- » Comparing policies or instructions issued and systems status and attributes by country, system area, policy area, responsible IT or legal staff, or other grouping to detect mismatches or misalignment

- » restrictions as defined by country or district law, evidence preservation requirements as dictated by a lawsuit or government investigation, disposal requirements or protocols as prescribed by country or district law, restrictions on transport as prescribed by country or district law, restrictions on processing as prescribed by country or district law

Unlike job ticketing systems or asset management applications that may be used in some IT environments, it's important to have a system that provides an accurate and dynamic link between the legal and compliance activities of the company and the IT staff that must adhere to legal obligations. Arguably, this IT governance center must be checked before completing many of the job ticket and asset management activities IT staff must do in order to ensure that there are no over-riding legal instructions on the data or system in question. Most job ticketing systems are task organization tools and asset management systems that also lack key capabilities for legal governance:

- » Status lookup and continuous display of ongoing obligations (such as holds) for which there is no determinate completion date

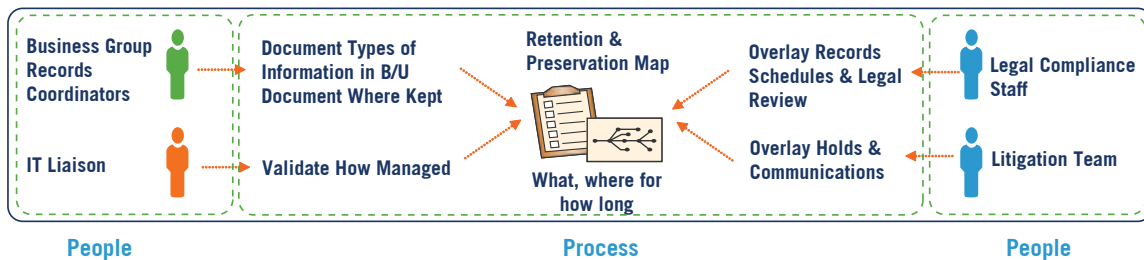
- » Any notion of legal duties, policies or instructions and any context of attorney-client communications
- » Management of attributes necessary to legal compliance such as capacity to preserve data, method and ease of collection
- » Ability to automatically link the appropriate retention schedule to a system
- » Dynamic communications and process transparency with the other stakeholders on the legal landscape
- » Ability to assess the current and historical burdens of discovery for a system or for a business unit and its systems

Having a purpose-built system for all the stakeholders in legal governance will enable the flow of information to be automated with little effort required to keep all stakeholders on the same page. A change in the IT environment is readily

apparent to legal, a change in a retention schedule readily apparent to IT, and a continuing hold obligation over system data is automatically visible to IT. No one party is burdened with updating the other and there are no “cracks” to fall through.

When companies have high volumes of systems and of data combined with high volumes of litigation, direct linkage and active management between legal and IT are essential to reducing risk and cost. Without this linkage, legal depends too heavily on IT infrastructure and process that may not exist; IT is left with a management burden it can't easily track combined with the responsibility to ensure success for legal processes they don't fully understand. Worse, they are tasked with managing data that is purely cost and risk to the company because they lack clear instructions on what can prudently be disposed in the face of ever-escalating pressures to reduce operating costs.

Technology Enabling People and Process



About CGOC

Founded in 2004, the CGOC is a corporate practitioners' forum uniquely focused on retention, preservation, and privacy. Its charter is to create a forum in which legal and compliance executives can get the insight, interaction, and information they need to make good business decisions. CGOC participation is limited to corporate managers and executives with responsibilities for litigation, discovery, and retention and records management, and to professionals who have specific expertise in these areas. For more information and to join CGOC, visit www.cgoc.com.

About the Author

Deidre Paknad
President & CEO, PSS Systems, Inc.

Deidre leads PSS Systems and is the innovator behind the company's visionary Atlas legal holds and retention management software. She founded the CGOC in early 2004, is a member of the Sedona legal holds and legacy data teams, and is a recognized subject matter expert on legal holds and enterprise retention management. She is a seasoned software entrepreneur and executive.