Governing Information Efficiently to Manage Costs and Litigate Effectively

It is widely accepted that the *volume* of information in the world doubles every two years, and this increase has forced businesses to reassess information management. However, the problem is not limited to Gigabytes. Instead, the pace at which information is generated and consumed (its *velocity*) and the explosion in new types of information (its *variety)* weigh heavy on modern business. These "Big V's" of big data[1] have strained legacy business practices related to information management. Record retention practices – which often involve manual comparison of records to a rigid schedule – have been rendered inadequate. As a result, businesses have become awash in redundant, obsolete, and trivial (ROT) information that threatens productivity, creates compliance risk, and complicates litigation. In addition, businesses are facing an unprecedented increase in cybersecurity threats and regulatory controls affecting how they must store, protect, and dispose of the information. Frustratingly, the emergency of these challenges has coincided with industry's near elimination of the administrative support that was once responsible for keeping records in order.

In short, the venerable records retention policies, which were originally developed to allow an army of administrative professionals to manually cull documents, no longer work. Instead, businesses are developing a governance framework that integrates recordkeeping, cybersecurity, regulatory, litigation, and operational requirements into processes that leverage technology to control the information lifecycle in a way that maximizes value while meeting legal obligations and mitigating risk. This field is known as Information Governance.

[1] *See* Doug Laney, "3D Data Management: Controlling Data Volume, Velocity, and Variety," Application Delivery Strategies (META Group), February 6, 2001 (available at https://www.gartner.com/). Since Laney's first description other commentators have added a myriad of other "V"s, but these three remain the most often cited.

For the litigator, a well thought out Information Governance program can simplify discovery, reduce spoliation risks, and lessen the likelihood of an obsolete document being weaponized by opposing counsel. However, to fully deploy this benefit, we must first be prepared to engage our client (and the court) in a thoughtful discussion of information workflows, process automation, and how these new tools can be harnessed to meet legal obligations.

What is Information Governance?

Information Governance ("IG") is the specification of decision rights and an accountability framework used to ensure appropriate behavior in the valuation, creation, storage, use, archiving, and disposition of information.[2] Often IG is implemented through an organization's development of programs designed to reduce risk, ensure compliance, lower costs and, most importantly, increase employee productivity. IG addresses records and information management, litigation readiness, and the control of private and sensitive information maintained by an organization. In its simplest form, IG combines traditional record and information management programs and employee productivity into real-world strategies that are easier to implement than traditional programs and are executable by even the most complex of enterprises. These programs allow organizations to better maintain, manage, secure, and dispose of their information through cross-functional initiatives.

Why do enterprises need to develop and implement Information Governance?

Traditional programs designed to separately maintain records, discovery, privacy, and other electronic information are becoming increasingly ineffective in a world where paper documents are becoming few and far between. With increasing data volumes, stringent legal and

[2] *Information Governance Primer for In-House Counsel,* Association of Corporate Counsel- Contoural, (2019), pg. 6.

regulatory recordkeeping requirements, and stricter privacy rules, organizations need to reorganize their data management programs to more effectively control both incoming and outgoing information. Comprehensive IG programs combine and restructure traditional programs with an organization's individual productivity needs to aid in the management of both paper and electronically stored information.

Recent studies show that the average corporate employee sends and receives more than 100 emails a day, with nearly 25 percent including attachments of some sort.[3] Another study from the University of California, Berkeley, indicates that nearly 96 percent of information stored by a corporate organization is preserved in a digital format.[4] Too many documents and too much data routinely cause problems with file management, which in many organizations is shared amongst hundreds of employees across desktops and other repositories. In addition to the record keeping issues, this glut has imposed an enormous toll on worker productivity, with industry analysts finding that up to 50% of an employee's workday is spent searching for information or recreating lost work product.[5] And, the trouble doesn't stop there. A recent survey found that approximately 86% of electronic records held by companies are either redundant, obsolete, trivial, or unknown in nature, and the global cost of storing this data runs into the 100's of billions of dollars.[6]

Federal, state, and industry-specific requirements likewise require organizations to maintain and enforce increasingly complex record keeping programs. The average U.S. corporation must comply with upwards of 30,000 legal and regulatory requirements, many of which require the retention of documents that are otherwise irrelevant, redundant, or obsolete.[7]

[3] "Metrics Based Information Governance," *White Paper* (2013), http://www.contoural.com/whitepaper_summary.php?id=28.
[4] "Information Governance Primer for In-House Counsel," *Association of Corporate Counsel- Contoural*, (2019).
[5] *The State of Data Discovery and Cataloging,* IDC (2008) (https://pages.alteryx.com/IDC-Info-Brief-Data-Discovery-Cataloging.html).
[6] Pedro Hernandez, *Enterprises are Hoarding 'Dark' Data: Veritas*. Datamation (October 30, 2015).
[7] Forrester. Security Concerns, Approaches and Techology Adoption. December 2019.

The continuing accumulation of both paper and electronic information poses a particularly unique challenge when an organization faces discovery in litigation. Increasing volumes of information pose the risk of organizations becoming non-responsive to discovery as they are forced to spend time, money, and resources combing through thousands of files, paper bins, *etc*. to respond to a single discovery request.

Most importantly, the larger the volume of information stored or maintained by an organization, the higher the risk posed by a potential data breach. Criminal groups and activist disclosure organizations often target and breach those organizations with a large client base and vast amounts of electronically stored financial or personal information. Breaches likewise threaten an organization's control and ownership of its intellectual property and internal strategies. Unlike IG, traditional "siloed" programs fall short in addressing these corporate concerns as responsibility for the maintenance of information is too often spread across individual business units. For example, an organization's IT department may be responsible for the management of data storage but not the actual content. The same organization's records department may be responsible for handling official records but have no direct role in the management and control of non-record documents or electronic information. The average employee who is responsible for the creation of electronic information is likewise likely unaware or indifferent to how files are managed throughout an organization's various units. This example highlights how disjointed initiatives and a lack of coordination between groups can lead to business practices which are wasteful and have the potential to result in the ineffective maintenance of information within an enterprise.

IG programs seek to combine each of these risks and realities into one structured program that centralizes responsibility, defines individual tasks, emphasizes employee productivity, and effectively controls the flow of information that is essential to an organization's business.

Records Policies and Retention Schedules and Litigation.

Record policies and retention schedules (RRS) are an essential component of an IG program. In the context of litigation, the generally accepted advice has been that a well-designed RRS should be simple, legally compliant, and rational – and therefore defensible. However, in the automation heavy IG world, litigators must be ready to develop a deeper understanding of records retention that involves information workflows, data-classification, and process automation that often utilize sophisticated artificial intelligence to make record keeping decisions.

For example, many businesses have begun "tagging" their unstructured documents to enable advanced functionality. Through tagging, metadata is added to individual files to identify security, compliance and retention requirements for each record. These tags can be manually applied by employees when a file or saved or they can be automatically applied by workflow tools or advanced "crawlers" that search through vast quantities of electronic files and tag them according to predefined heuristics. Once tagged, additional technologies can be employed to allow for automated preservation and disposition, thereby ensuring greater compliance with complex record-keeping requirements that have often been seen as too unwieldly for employees to manually follows. However, to ensure defensibility, data classification (along with its retention tagging) must meet regulatory and legal requirements, must conform to the company's record retention schedule, and must be described clearly and succinctly for the courts to understand.

In addition, where manual data-tagging is used, companies should simplify policy and tagging requirements to create big buckets for records categories. While this may result in the retention of some records for a longer period than is absolutely necessary, that consequence

should be outweighed by the increased useability for employees when categorizing and locating records within the system. Simplicity is also achieved by articulating clear and concise category descriptions that minimize the need for operations-level employees to decide what records should and should not be preserved.

Finally, good RRS should distinguish from "Records" (with a capital 'R') that must be preserved to meet legal requirements from documents that should be preserved to meet a business objective but can be destroyed when they no longer have business value. Specifically, some record retention periods are mandated by state or federal law and therefore it is incumbent upon the business to identify and to comply with those requirements. For example, certain employment records, workers' compensation records, environmental records, tax records, and safety-related data are subject to specific government-mandated retention periods.

For those records (with a little "r") having no legally required retention period, an RRS will withstand adversarial or judicial scrutiny if it is found to be reasonable. If there is a rational basis for the overall architecture and particular components of the RRS, then it should satisfy the "reasonable" test.

Other features that will contribute to a legally defensible RRS include:

- Being updated periodically to reflect changes in the law and in the business itself.
- An individual or team charged specifically with monitoring compliance (including deletion of records after expiration of their retention period) or use of a third party service to monitor same.
- Enforced consequences for violation of the RRS.
- An individual or team responsible for preparing and communicating legal holds and related communications.

Commented [CG1]: This isn't feasible in practice, and technologies such as in-place preservation make it unnecessary.

From a litigator's perspective, digitizing (in searchable format) as many paper records as possible is also beneficial. Doing so will minimize the chance of inadvertently losing or destroying relevant materials, maximize the scheduled destruction of stale records, and aid in the search for relevant records in response to legal hold notices and discovery requests.

Also, any company policies and procedures to be retained pursuant to the RRS should be consistent and properly vetted. It is not unusual for companies to have a multitude of written policies and procedures (hundreds even) addressing a broad variety of subjects. It is also not unusual for those policies and procedures to sometimes conflict with one another (especially if created within the silos of discrete business units), or to inadvertently include provisions that are not legal (*e.g.*, in violation of the Americans with Disabilities Act). Further, policies and procedures should be written in such a way that they are readily understandable to the persons who are expected to comply with them. Legalese and unnecessary complexity are unhelpful.

How are Courts Addressing Information Governance?

Courts are increasingly willing to analyze the integrity of IG systems when deciding whether to impose sanctions for evidence spoliation. And, while the 2015 amendment to FRCP 37(e) has reduced the risks of harsh sanctions for failing to preserve ESI[8], the failure to have an RRS that is simple, legally compliant, and rational can result in significant undesirable consequences. One example is found in the case of *Phillip M. Adams & Associates, LLC v. Dell, Inc*., 621 F.Supp.2d 1173 (D.Utah 2009), which involved patent infringement. Essentially, the plaintiff moved for default judgment against two defendants for alleged spoliation of evidence

Commented [CG2]: I don't think we want to talk about ESI spoliation without acknowledging the change to FRCP 37(e).

[8] While Court's have shown a mixed reaction to FRCP 37(e)'s new "intent to deprive" requirement for imposing sanctions, recent decisions do indicate a move from the imposition of case-dispositive sanctions to measures sufficient to cure any prejudice that resulted from the spoliation. *See* S. Himmelhoch & N. Ben-David, *Rule 26 Proportionality: Have the 2015 Amendments Brought Common Sense to the Preservation Obligation?*, 68 DOJ J. Fed. L. & Prac. 81, 88 (2020)

(primarily source codes, programs, and emails). After considering the evidence regarding the defendants' lack of a reasonable RRS and inability to produce certain materials, the Magistrate Judge concluded,

> …[Defendants'] system architecture of questionable reliability which has evolved rather than been planned operates to deny [Plaintiff] access to evidence. This should not be excused. [Defendants] did not have a designed information management policy taking various needs into account. 'An organization should have reasonable policies and procedures for managing its information and records.' 'The absence of a coherent document retention policy' is a pertinent factor to consider when evaluating sanctions. Information management policies are not a dark or novel art. Numerous authoritative organizations have long promulgated policy guidelines for document retention and destruction.

Id. at 1193-94 (footnotes omitted). The Court made clear that the Defendants' RRS fell short of the legal standard:

> [Defendants'] practices invite the abuse of rights of others, because the practices tend toward loss of data. The practices place operations-level employees in the position of deciding what information is relevant to the enterprise and its data retention needs. [Defendant] alone bears responsibility for the absence of evidence it would be expected to possess. While [Plaintiff] has not shown [Defendant] mounted a destructive effort aimed at evidence affecting [Plaintiff] or at evidence of [Defendants'] wrongful use of intellectual property, it is clear that [Defendants'] lack of a retention policy and irresponsible data retention practices are responsible for the loss of significant data.

Id. at 1194. Although the Court did not grant the motion for default judgment, it did conclude that Defendants had violated their duty to preserve information and that a sanction was appropriate. However, the degree of prejudice and appropriate sanction could not be determined until after discovery had closed.[9] Although ultimately the Defendants avoided entry of a default

[9] The trial judge subsequently ordered an adverse inference sanction for spoliation of evidence, although the Federal Circuit Court of Appeals reversed because 10th Circuit law required a finding of bad faith for such a sanction and the trial court had not made that determination.

judgment, the issue had a significant negative impact on the direction of the lawsuit and the cost of litigating the spoliation claim was substantial.

Particularly in lengthy litigation, the sanctions associated with evidence spoliation can be severe. *DR Distribs., LLC v. 21 Century Smoking, Inc.*, 2021 U.S. Dist. LEXIS 9513; 2021 WL 185082 (N.D. Ill. Jan. 19 2021). The *21 Century Smoking* case involved trademark litigation that spanned more than eight years. *21 Century Smoking, Inc.*, 2021 U.S. Dist. LEXIS 9513 at *7. At an in-person status conference, the district court learned that defense counsel never issued written litigation holds to the defendants in the case. *Id.* at *7. At the conference, the court also "asked the parties how they intended to search for ESI, whether through search terms or predictive coding/technology assisted review." *Id.* at *8. Time passed and the plaintiff eventually moved for sanctions relating to the failure to timely produce ESI and for the spoliation of ESI. *Id.* at *9. The plaintiff sought a "full arsenal of sanctions weapons," including civil contempt, inherent authority, defaulting the defendants, and dismissing the defendants' counterclaims. *Id.*

Although the court did not impose the most serious sanctions of default or dismissal, it barred defendants from using any undisclosed information or contesting certain facts and ordered that the jury would be informed of the failure to provide documents and to preserve ESI, that defendants pay plaintiff's attorneys' fees and costs related to the sanctions motions, and that the defense counsel complete at least eight hours of continuing legal education on ESI. *Id.* at *11–*13. The court did not impose monetary sanctions because "it would likely result in frivolous motion practice, based on claims that the monetary sanction was punitive rather than compensatory." *Id.* at *15.

Courts today expect parties not only to have an established IG system, but to inquire of the IG systems used by witnesses and opposing counsel as well. *Thomas v. Randall Chambers God's Way Trucking, LLC*, 2019 U.S. Dist. LEXIS 231247 (E.D. La. May 15, 2019). In *Thomas*, the defendants in a vehicle collision case moved for contempt for failing to properly respond and provide documents requested pursuant to a subpoena *duces tecum*. *Thomas*, 2019 U.S. Dist. LEXIS at *2. The subpoena sought production of medical records, finance agreements, billing information, and diagnostic reports and films. *Id.* at *3. However, the production did not contain any finance agreements. *Id.* The court noted that during the deposition of the plaintiffs' treating physician, the defendants did not question the physician about the IG system "to ascertain if all the electronic communications are contained in one system or if there is a separate email system." *Id.* at *13–*14. Finding no clear attempt by the physician to avoid compliance with the subpoena, the court declined to impose sanctions for contempt against the physician. *Id.* at *15. However, the motion also sought contempt against the medical company. *Id.* at *16. With regard to the medical company, the court ordered that the failure to respond to a subpoena warranted a finding of contempt. *Id.* at *19.

Finally, retaining records *beyond* a legally required or reasonable time period can also have adverse legal and business consequences. Generally, information loses value over time and increases in risk – it loses context, is subject to collateral attack for tone, meaning, prejudice, and cultural sensitivity, and is subject to changes in "reasonableness."[10] Moreover, genuinely problematic records will persist. Infamous examples of such records include internal memos written by employees of Brown & Williamson (in 1963, regarding the addictiveness of nicotine and the adverse physical affects of smoking cigarettes) and Ford Motor Company (the so-called

[10] One only need look at the term "asbestos", which was hailed as a wonder material in the 1950s and is met with absolute fear and revile in a modern court.

"Pinto Memo" in 1968, providing a cost-benefit analysis of proposed safety regulations and concluding that the dollar cost of compliance would vastly outweigh the "savings" that would result from the avoidance of fiery deaths and serious injury). While no one is endorsing corporate malfeasance or irresponsibility and these documents represent extreme examples, they may have never seen the light of day had they been controlled by a well-designed and executed RRS.

Engaging your client on the topic of Information Governance.

While the importance of sound IG policy cannot be understated, it may be difficult for outside counsel to know where to begin when representing a large and sophisticated client. At the outset of complex, fact intensive litigation, counsel should start with the basics:

- Does the organization have a data inventory available (a.k.a. a "data map") to help locate potentially responsive information?
- Does the organization employ a data classification scheme that can be used to locate responsive information?
- Are potentially responsive data sources governed by defined information workflows, automation, or automated tagging?
- How does the organization employ preservation and collection strategies across relevant portions of its data map?
- And, what is your strategy for handling unmapped data?

Many of these questions will naturally flow into the questions of eDiscovery and how preservation and collection specifications can be developed to address the data landscape, but counsel will be much better armed to address those questions if they understand the basics of Information Governance.[11] In the end, a client that can answer these questions will be well on their way to governing information efficiently to manage costs and litigate effectively.

[11] *See Electronic Discovery Reference Model*, EDRM.net (2021).