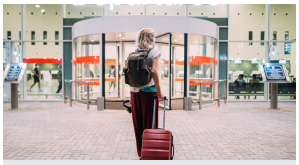
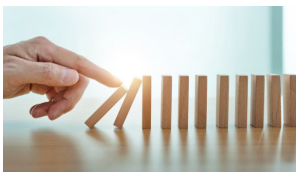
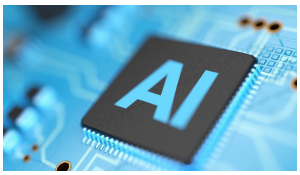
2022 Blog Book



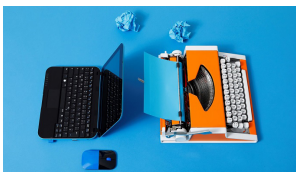


epiq angle

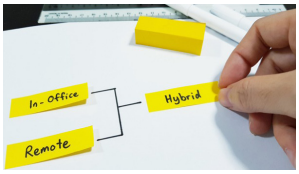




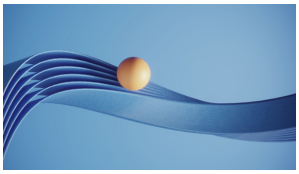

















epiq contents

The Epiq Angle brings you our thinking on topical issues in eDiscovery, bankruptcy, corporate restructuring, data breach response, global business transformation solutions, class action, and mass tort administration.

epiq contents

epiq contents

Looking Back at Data Privacy Developments in 2021: Part One – the U.S.

With the start of a new year, it is the perfect time to reflect on major legal movement with consumer privacy last year both in the U.S. and abroad. Data privacy is a hot issue that will continue to trend as more countries shape their privacy landscapes, established regulatory bodies issue fines, and seminal case law unfolds. 2021 was a pivotal year in this space with new or proposed legislation in several states, large General Data Protection Regulation(GDPR) fines, instructive case law, and important cross-border activities. Below are some major data privacy developments in the U.S. to ponder and prepare for what is to come in 2022. Part two of this blog series will be released next week and will round up last year's major international privacy updates.

Lack of Federal Legislation

In 2021, there was still no significant movement towards creating a comprehensive U.S. federal consumer privacy law. The recent wave of state legislation, more global laws with extraterritorial effect, and continued reliance on digital platforms that collect personal data may accelerate the creation of a new federal privacy framework. However, the struggle between lawmakers and lobbyists coupled with the historically slow legislative process could keep delaying meaningful federal activity in this space. For now, the federal government continues to regulate data privacy in a piecemeal fashion through already established legal frameworks like healthcare and credit reporting laws or Federal Trade Commission enforcement.

New State Legislation

There was a flurry of privacy-related activity in the states last year. Virginia and Colorado joined the ranks of California and passed comprehensive data privacy legislation. Virginia's law becomes effective in January 2023 and Colorado's in July 2023, so organizations should use this year to review the laws and update compliance plans. Other states enacted laws touching on specific areas of privacy like Nevada allowing consumers to opt out of information sales to data brokers or Utah providing organizations with a limited safe harbor for data breach notification. Legislators also introduced privacy bills in 21 additional states that offered varying of degrees of consumer protection. While several did not make it, bills in Massachusetts, Minnesota, New York, North Carolina, Ohio, and Pennsylvania remain on the table this year and are in committee.

The three active consumer privacy laws grant similar protections such as the right to access, correct, or delete data; opt-out of sales; and portability. These states also require organizations to provide notice to consumers regarding collection of their personal data. Even with many similarities, there are some unique differences that will affect compliance approaches. Here are some big ones to note:

- **Enforcement**: California is the only state that currently allows for a private right of action. The state also gives the Attorney General (AG) and newly formed privacy agency enforcement powers. Virginia only delegates enforcement to the AG and Colorado allows the AG and District Attorneys to seek penalties for privacy violations. California's private right of action is limited to instances where data breaches occur, so it will be interesting to see if any future state laws expand on this right.
- **Grace Period:** The laws also grant organizations the right to cure violations before the appropriate enforcer can seek penalties via an enforcement action – 30 days for Virginia and 60 days for Colorado. While the California Consumer Privacy Act (CCPA) also grants a 30-day cure period for enforcement actions and civil suits, when the stricter California Private Rights Act (CPRA) becomes effective in

2023 this allowance will only remain when a consumer initiates a private right of action. After that, when the AG or California privacy agency find noncompliance, they can immediately start up an enforcement action.

- **Data Protection Assessments and Sensitive Data:** Like the GDPR, both Colorado and Virginia require that controllers perform data protection assessments for high-risk processing. California does not share in this requirement. Colorado and Virginia also directly track some key GDPR language, like the definition of sensitive data. Both states also grant an opt-in right for consumers regarding processing sensitive data, while California does not.
- **Treatment of Employment-Related Information:** The CCPA broadly defines consumers and will specifically apply in employment situations when the even stricter CPRA becomes effective in 2023. Conversely, Virginia and Colorado exclude employment data from regulation.

Although this list highlights the critical differences between these three laws, it is not exhaustive and organizations should consult with their counsel and provider partners to ensure policies and procedures align with compliance initiatives. Remember that these laws can apply outside of state borders if an organization does business there.

California Enforcement Activities

In 2021, CCPA enforcement gained some speed. Last July, the AG released a report detailing the office's non-compliance notices. Violations included insufficient privacy policies, untimely responses to CCPA requests, and much more. Most of the organizations remedied within the 30-day cure period and avoided enforcement actions, but about 25 percent remained under investigation or were still within the right to cure deadline at the time of the report. There have not yet been any fines. With the recent creation of the California Privacy Protection Agency and the stricter CPRA that removes the cure period becoming effective next year, even more vigorous enforcement and fines are likely on the horizon.

In 2021, there were also a handful of civil suits resulting from data breaches or that cited CCPA protections. While there have been no pivotal rulings yet, affected organizations and the legal community should continue to watch if any cases result in significant penalties. However, this will probably not gain much traction until after the CPRA becomes effective in 2023 and stronger protections unfold.

Conclusion

It is a confusing time for organizations that process U.S. consumer data, as privacy-related obligations can change quickly as more states pass laws. Overall, the active state laws and bills proposed during 2021 lack uniformity in several key areas such as the definition of consumer or personal data, the ability to initiate a private right of action, consumer rights, and various obligations for organizations. This will inevitably spark confusion and legal battles down the road for organizations operating in multiple jurisdictions. For now, one solution is to model compliance plans around the strictest state privacy rules that apply and incorporate flexibility for situations implicating unique responsibilities if and until a federal standard emerges. Organizations already subject to the GDPR will have a good foundation to work with when navigating U.S.-related obligations but will need to make sure unique provisions are upheld pursuant to the individual state law.

For more information about U.S. privacy law consider reading U.S. Data Privacy Roundup – What is on the Horizon?

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Privacy Roundup Part Two: Significant International Updates

Last week's blog detailed the wave of state legislation that occurred in the U.S. during 2021. It is no surprise that there were also many data privacy developments abroad. It is crucial that organizations affected by international laws, regulatory actions, or court decisions stay informed and determine any influence on business practices and compliance efforts. The global privacy revolution can create new and sometimes conflicting responsibilities. Below is a summary of key international data privacy activity, including some best practices to improve compliance management efforts.

International Legislation

Several countries around the globe took steps to tighten consumer privacy regulation. The first round of amendments to Singapore's privacy law became effective on Feb. 1, 2021. The law now grants consumers a private right of action, mandates data breach notification to the Personal Data Protection Commission in proscribed circumstances, expands the definition of deemed consent, and enacts new categories of actions that can result in criminal punishment. Other substantial revisions will occur later this year.

China also passed new privacy regulations. The Data Security Law fills gaps present in the country's cybersecurity framework and broadly applies to processing activities related to personal and non-personal information that could affect national security, public interest, or lawful consumer rights. The Personal Information Protection Law more closely mirrors the EU's GDPR and regulates personal information processing. Chinese consumers now can access, correct, and delete information. Data controllers are responsible for conducting impact assessments and there are restrictions on cross-border data transfers. Both laws are now effective and can result in heavy fines.

Canada's proposed national privacy law remained in legislative process last year. If passed, the law would grant consumers control of their data and ensure organizations are more transparent about how they handle personal data. Although the national law is still underway, Quebec adopted its own privacy law with extraterritorial reach to increase protections and management over personal and sensitive information. Some key provisions include mandated data

governance policies and procedures, consumer right to data portability, consent for data collection, and transfer restrictions. Noncompliance can result in administrative penalties of $10 million or more, penal proceedings that can result in fines of $25 million or more, and private lawsuits. While the law went into force last September, certain provisions will be phased over a three-year period.

Some other countries where data privacy laws became effective last year were Belarus, South Africa, Uganda, and Panama. This list is not exhaustive but illustrates the global privacy trend is not losing speed. Additionally, as of last August Brazil's enforcement agency can issue administrative sanctions under the country's newer privacy law. The agency indicated it would investigate thoroughly and levy fines when necessary. Organizations can look to guidance issued last May to inform compliance-related decisions and help avoid penalties. Several other countries passed or updated laws, or have crucial changes planned for 2022 and 2023, so it is important for organizations to monitor developments in any geographic location where they conduct business or handle personal data. Some best practices to manage varying domestic and global privacy compliance requirements include dedicating staff to create and maintain compliance plans, regular training, cybersecurity audits, and data mapping. Taking these measures can reduce risk of unprotected data and bolster compliance initiatives.

GDPR Cross-Border Data Transfers

A landmark court decision in July 2020 caused the European Commission to issue new standard contractual clauses (SCCs) this year applying to personal data transfers from EU member states to other countries. In Schrems II, a consumer activist filed a case against a big tech company regarding data transfer policies between the U.S. and Ireland, which he argued were risky. The court held that SCCs were insufficient when a country does not offer the same level of protection and consumer rights as the EU. Cross-border data transfers are only valid under the GDPR when adequate safeguards are in place to secure the data. Without an adequacy decision in place and prior mechanisms deemed invalid, the U.S. has been in limbo. Affected organizations have been waiting to see how the European Commission would alter the longstanding SCCs, as this is one of the most common ways that cross-border data transfers from the EU occur not only in the U.S. but all over the globe.

The new SCCs focus on enhanced accountability and transparency to ensure all transfers to the U.S. or other countries deemed inadequate align with the GDPR's privacy standards. Some key features include four modular clause options, mandated data transfer impact assessments, and authorization of multi-party agreements. The new SCCs also do not restrict the physical location of the data exporter to an EU country. Organizations required to use SCCs for data transfers need to review the new requirements and create policies that will streamline future transfers. The old SCCs were repealed on Sept. 27, 2021, but already established clauses will remain effective until Dec. 27, 2022. Prior to this date, organizations should modify their contracts and provide appropriate notices to remain compliant.

GDPR Fines

2021 was a year of rigorous GDPR enforcement, with big tech companies being noticeably impacted. In July, the Luxembourg data protection supervisory authority levied its largest fine to date, for over 700 million Euros. The previous record high was 50 million in 2019. This decision has been appealed and in December, a Luxembourg judge struck down recent orders from the data protection authority saying the company would face extra daily fines for failure to implement consumer data process changes by a certain date as the judge found the authority's directives on what needed to change to be unclear.

The second highest fine last year was levied in Ireland for 225 million Euros for deficient consumer notice about data processing practices in privacy policies. Last year, there were also nearly 20 other fines over 1 million Euros.

Two things to watch out for this year are whether heavier fines keep trending and if any appeals result in complete reversals or significant fine reductions, as this will be influential in future enforcement actions. The intermediary decision against the Luxembourg data protection supervisory authority already illustrates that additional penalties will need to be sufficiently warranted.

Being the first to comprehensively overhaul data privacy regulation, the EU has seen the most enforcement action in this space. However, with new laws carrying heavy fine potential now active in places like China, Brazil, and Canada it is crucial to monitor emerging global enforcement trends.

Large regulatory fines are also happening in other contexts, including competition. Just like the potential for big tech organizations to obtain and mishandle sensitive information is a major reason for global focus on data privacy, these organizations also hold the ability to significantly hinder market competition. In December 2021, the Italian competition authority imposed a fine of over 1 billion Euros on a company for favoring merchants that used their fulfillment services and hindering sales for other organizations. It will be interesting to see big tech's response or any changes to current policies and practices as larger fines continue with regards to privacy and competition.

Conclusion

With each year that passes since the GDPR's creation, more countries reform data privacy landscapes. It will be interesting to see how enforcement affects compliance, as more organizations monitor trends and tweak compliance programs accordingly. In addition to deploying internal compliance efforts, a provider familiar with data privacy updates that can implement information management tools, detect security shortcomings, and orchestrate compliance plans can be a beneficial resource.

To learn more about data privacy, consider reading part one of this blog.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Three Data Trends to Watch

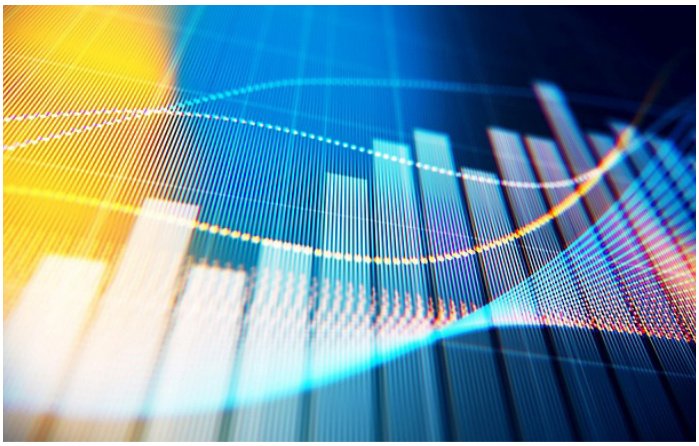
Each year, practitioners and the courts face data issues applying to collection, preservation, security, compliance, global practice challenges, and more. Some questions repeat or evolve, while others are entirely fresh stemming from emerging technologies or new digital habits. Attorneys must keep tabs on these matters and implement practice changes where necessary to remain effective, ethical, and compliant. Below are some key data trends from last year that will continue to develop in 2022 and reflection on how they influence eDiscovery expectations.

The Rise in Virtual Proceedings

While remote court was not a foreign concept prior to the pandemic, most jurisdictions did not include it in their regular operational models and only allowed it on occasion. Traditional in-person attendance for significant case events was the norm. Now, courts across the U.S. and the globe have realized how beneficial virtual proceedings can be when used for appropriate matters. Many facets of a civil case can be managed virtually – at least to some degree – which offers cost and time saving advantages to everyone involved in the process. This includes digitizing court appearances, motion hearings, courtroom directories, and more.

The remote court trend will continue in 2022 but the role it plays will vary depending on jurisdictional preferences. It is a safe prediction that usage will also be scaled and heavily rely on case factors. So many cases have faced delays and courts are still under capacity restrictions. Jurisdictions that continue to integrate virtual models into practice will help lessen some of this burden, but lawyers should continue to expect discovery delays until the backlog clears and expectations settle. Best practice during transitional periods like this is to factor additional discovery and case costs caused by delays into settlement evaluation. Using artificial intelligence (AI) tools for early case assessment can help predict costs and provide valuable insights on which cases should settle and which should weather the storm.

It is also important for practitioners to understand and prepare for discovery challenges that virtual court imposes. For example, with remote depositions an ongoing challenge has been how to present exhibits to a witness at the appropriate



time. Depositions are often about strategy and provide the lawyer requesting them with the opportunity to carry out questioning in a certain way. Providing access to exhibits too early on can hinder this. Many have turned to solutions where the court reporter can control exhibits and present them in real time. Another option is having the deposing lawyer send the exhibits via chat features on the collaborative platform. Some jurisdictions have started testing remote jury pilot programs, so this would be an important tool to consider for trial exhibits if faced with a virtual or semi-virtual trial.

Emerging Technology

This is a multi-faceted and ever-evolving trend. With the continued rise in remote working and reliance on collaboration platforms across many industries last year, unique challenges presented at every step of the eDiscovery process. Most notable were preservation and collection concerns. Simply being aware of issues new data sources bring to the table helps contemplate where critical information may exist to determine if there will be any obstacles with retrieving, processing, and reviewing data.

Common challenges stem from working on personal devices lacking sufficient security, absence of strong device or app policies, data disappearing from dynamic chat or file sharing platforms, lack of standardized data formats, missing content, communication not in chronological order when retrieved, increased usage of things like emojis that invoke contextual

review, and scattered data storage. Some resources to combat these obstacles include solutions that can collect and group messaging data to preserve context, archiving tools, partnering with providers with forensic expertise in collecting unstructured data while preserving chain of custody, and data mapping. Also remember that factoring in data trends and challenges at every step of the EDRM can have a positive downstream effect. This starts with strong data policies and information governance initiatives that evolve as communication habits or application preferences change.

With emerging technologies and eDiscovery, thinking more about the requesting party's role can also increase efficiency in future matters. To be more effective, lawyers should contemplate what details to include in eDiscovery requests and anticipate obstacles that opposing counsel may face. Crafting requests in a more targeted fashion will provide better access to desired data. Court decisions on eDiscovery disputes in the space, specifically when it deals with emerging technologies that are harder to collect or review, will provide pointers on crafting requests to remain compliant and get what is needed for the case.

Emerging technology's influence on eDiscovery will absolutely persist. One prediction is that there will be an increase in managed services partnerships to promote cost predictability, legal defensibility, and access to superior technology to combat collection or review hurdles.

Keep an eye out for any privilege developments in 2022, as this has been an unchartered area needing attention for years. Creating, producing, and reviewing privilege logs has historically been a daunting task and many have called for the need to reform outdated practices associated with this process. Some trends that could accelerate include the use of AI to limit the burden of privilege review or increased collaboration between parties about what information can be excluded from logs.

Legal as a Value Center

Legal transformation started to accelerate last year, as many placed higher emphasis on ways to make legal more valuable to the entire organization. This is a slow-moving trend that will keep gaining speed, but it is important to analyze how eDiscovery fits into the puzzle even at early stages of transformation initiatives. Litigation has and will always be one of the top areas legal departments spend their money, as eDiscovery and other case needs can prove to be very costly. Some practices to continue in 2022 that will guide transformation efforts include enhanced information governance programs, partnerships with full-service eDiscovery providers, yearly litigation-focused spend analysis, and metrics evaluations. Tapping into resources like this illuminates areas requiring attention and increases legal's overall value, which culminates in cost-savings and risk reduction.

To learn more about the adoption of TAR, click here.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Five Significant eDiscovery Rulings from 2021

At the beginning of every new year, it is important for legal teams to reflect on key eDiscovery case law from the year before that will influence future processes and case strategy. In 2021, the U.S. courts handled a variety of eDiscovery issues – some were variations or progressions of topics debated in the past while others involved new obstacles stemming from emerging technologies. Key themes included aligning sanctions with the realities of emerging technology, continuing focus on proportionality, the pandemic's influence on eDiscovery protocols, increased attention to Federal Rule of Evidence (FRE) 502(d) disputes, and analyzing hyperlinks in the context of eDiscovery production mandates.

Here are five of the most interesting cases from 2021 and some major takeaways to guide similar eDiscovery obstacles in the future.

Federal Trade Commission v. Vyera Pharmaceuticals, LLC. S.D.N.Y. June 1, 2021

The main issue was whether deleted text messages warranted sanctions. During discovery, it became clear that a key custodian of Defendant pharmaceutical company was a former employee that was subsequently incarcerated. He kept the company phone after departure and transferred it to his family upon incarceration. Plaintiffs discovered that the phone was wiped in 2016-2017 and therefore they were unable to obtain any data. There was also a contraband phone involved where an executive of Defendant's company chatted with the former employee about matters relevant to the case via WhatsApp. This data was no longer available, as WhatsApp automatically deleted the messages.

Plaintiffs asked for spoliation sanctions in the form of an adverse inference. The court granted the motion as to the contraband phone. Through testimony of Defendant's executive, plaintiff established that the custodian discussed relevant business matters on this phone and knew WhatsApp would not preserve the data. Because the plaintiffs did not offer any evidence illustrating the failure to preserve relevant evidence on the company phone, the judge did not allow sanctions in that instance.

The major lesson from this case is that when evaluating sanctions courts are accounting for unique features of emerging technologies – especially when a platform enables surreptitious behavior. Additionally, to be successful on a motion for sanctions parties must put forth evidence that establishes the deleted or hidden communication existed. This can be difficult with ephemeral messaging apps that are designed to delete data after a certain time (often instantaneously). More courts are seeing this behavior and it is of the utmost importance that litigators can prove destructive actions occurred that interfered with eDiscovery – whether it be through witness testimony or other evidence documenting that the party communicated over another platform known for not preserving chats.

D'Agostin v. Fitness International, LLC D. Conn. May 12, 2021

The central issue here was defining proportional eDiscovery limitations regarding timeframe and geography. This was a slip and fall case at an LA Fitness gym locker room where plaintiff made an eDiscovery request for information on similar accidents occurring at nationwide locations during the previous five years. Defendants challenged this as lacking proportionality, and the magistrate judge ordered the parties to meet-and-confer to narrow the request. The parties could not agree – plaintiff narrowed down to four states over five years, but defendants stood firm on only producing

information from the state where the accident happened over three years. The judge agreed with plaintiff's reduced request and the defendant filed an objection with the district court, citing disproportionality due to facility differences in other states. The court overruled the objection with one caveat, which was to clarify that production only applied to incidents occurring in tile areas of a locker room. The judge found the reduced request proportional because it cut out over 600 facilities that the prior request encompassed. Also, that LA Fitness locations in other states had similar tiled areas to the incident at hand to establish constructive notice of dangerous conditions.

The main takeaways from this case are two-fold. First, this is one case of many from last year where the court prioritized proportionality. The potential for eDiscovery to blow litigation budgets and delay proceedings is high as the data generated daily continues to multiply. This has caused courts across the nation to spend more time analyzing proportionality disputes and limiting scope to control costs and manage time when possible. Second, while narrowing production requests is a standard eDiscovery dispute that is fact-dependent, the initial pivot to counsel cooperation illustrates the continuing trend starting well before 2021 of courts wanting parties to solve proportionality issues outside court whenever possible. This is also a cost and time saving tool allowing both parties to get what they need without wasting judicial resources on unnecessary motion practice.

Berkeley*ieor v. Teradata Operations, Inc. No. 17 C 7472 (N.D. Ill. Aug. 12, 2021)

Plaintiff filed a motion to compel various discovery processes – one being live deposition attendance requiring air travel. Due to personal scheduling conflicts, the attorneys demanded that the witness deposition occur on two days a week apart. This would mean that opposing counsel (located in Chicago) would have to fly out to California on two separate occasions to complete the deposition. The judge denied this motion and ordered it to be held remotely due to the ongoing risks imposed by the pandemic and lack of cooperation surrounding the notion that defense counsel should take two costly trips to complete the deposition. Plaintiff counsel's argument that the deposition needed to be live and assertions that the pandemic conditions had improved did not sway the judge, who commented that remote depositions have flourished for many years and physical presence of counsel is not always needed to ascertain truth or achieve justice.

The major takeaway from this decision goes deeper than the obvious conclusion that courts will grant ongoing flexibility during times of great uncertainty, such as a pandemic. It also illustrates the trend of courts allowing and embracing virtual processes as the norm, which has been accelerated the last two years due to necessity. In the short-term, litigators should expect and embrace flexibility when dealing with traditional in-person events that can be accomplished remotely – especially when dealing with significant travel. Looking past the pandemic, it is also safe to anticipate that courts will continue to allow for remote discovery processes more often – especially those that reduce costs and streamline case resolutions.

Klein, et al. v. Facebook No.: 20-cv-08570-LHK (N.D. Cal. June 3, 2021)

This matter involved resolution of several disputes stemming from FRE 502(d), which authorizes a party to proactively request a court order preventing privilege waiver when disclosure occurs. A central issue was whether to apply the order only to inadvertent disclosures of privileged information. While some district courts have done this, the judge here did not since the rule does not apply any such restriction. The judge instead mandated that the order include the maximum protection under Rule 502(d), which at face value blanketly applies to all types of disclosures. The judge also made sure to explicitly include that Rule 502(b) does not apply here, which is the default test when parties do not enter a 502(d) privilege protection order.

Parties have historically shied away from Rule 502(d) even though it offers widespread protection. For many, this is likely due to being uninformed about the rule's reach. Courts have begun to dive into some of the rule's nuances and last August, the Sedona Conference released commentary on why these orders should be standard practice in federal proceedings. The major takeaway here is that litigators should expect to see more Rule 502(d) activity this year both in general practice and around issue splits - like application scope or parameters around clawback notices. As Klein noted, no appellate court has yet weighed in on the inadvertent disclosure vs. blanket application debate. Future rulings by higher courts in this space will be very instructive.

Nichols v. Noom, Inc. No. 20-CV-3677 (LGS) (KHP) (S.D.N.Y. Mar. 11, 2021)

This decision centered on the issue of whether courts should view hyperlinks as attachments for the purposes of eDiscovery production. The parties agreed to use Google Vault to collect data in their ESI protocol. Upon review, plaintiffs discovered that a common practice was to include hyperlinks to internal files instead of physically attaching documents to emails. They motioned the court to compel defendants to use an outside vendor who could recollect hyperlinks as part of the document

family, as Google Vault did not have this capability. The magistrate judge denied the motion, finding extra costs and delays as disproportionate to the case and ordering plaintiffs to alternatively request from defendants any specific hyperlink documents not already produced.

What makes this decision intriguing is how the judge elaborated on the discussion of viewing hyperlinks as synonymous to physical document attachments. The judge recognized that including hyperlinks over physical attachments is now a common practice. However, she concluded they cannot be the same because a hyperlink will not always link to relevant information to a case, but a physical attachment would because it acts as an extension of the conversation. One example given was when someone hyperlinks contact information. She also commented on how the parties did not specifically mention hyperlinks in their ESI protocol. The district court upheld this decision but did not comment on the substance of the ruling, which leaves the door wide open for future opinions.

The major takeaway from this case is that for now, hyperlinks are not universally accepted as attachments. As courts get more technical education, there is a good chance this stance will change just as how other eDiscovery matters involving new communication preferences have evolved throughout the years. Future considerations will likely be around balancing the burden on receiving parties to associate separate documents to hyperlinks when determining if the production is missing key hyperlink data. Also expect future discussion on whether hyperlinks operate as modern attachments, since many jump to a relevant document stored internally on a cloud platform. This data would be relevant to production in numerous instances and demand unique collection efforts. Another takeaway from this case is the importance of protocol language. If the protocol clearly mentioned hyperlinks, the judge may have ruled differently. So, until the stance on the hyperlink debate solidifies a way to ensure proper production would be to reference modern attachments such as hyperlinks in the ESI protocol.

Conclusion

The topics covered in the above cases will evolve in 2022, as many deal with the modern issues associated with changing technology usage and remote processes. This includes eDiscovery disputes surrounding hyperlinks and other modern attachments that still require significant court intervention to solidify stances. Litigators should also pay close attention to new decisions involving Rule 502(d), as the recent commentary by Sedona Conference may spark increased adoption of this rule which will inevitably accelerate ambiguity issues to the courts.

Interested in learning more? To read related blogs from Epiq, click here.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Leveraging Technology and Transformative Tools to Support Law Firms with Global Needs

Globalization opportunities and expectations continue to arise around every turn. From organizations offering services outside their operational borders to the rise in remote hiring widening the job pool across the world, nearly every market now has some international elements. The legal industry is no exception, as many areas are influenced by globalization. Litigation needs include cross-border eDiscovery and international contracts or business deals; and law firms continue expansion into new territories.

It is interesting to look at this topic from the law firm perspective. The concept of globalization is not new in this space. For decades, large firms in places like the U.S. and U.K. have globalized in response to client needs expanding across borders. Many have done this quickly and thrived. Present day, more firms than ever before have several locations worldwide or partner with contracted counsel or providers holding competencies in countries where business needs arise. Today, the continued rise in digitization expands international needs and obligations for firms of all sizes regardless of whether they currently have a global presence. It is crucial to regularly evaluate what this means in terms of legal technology adoption and how to leverage the best solutions that refine global processes and allow firms to maintain a competitive edge through innovation.

Technology and Globalization

New technological needs and prioritization will result from a firm's cross-border activities. It is important to remember that demand and eventual adoption of a certain technology is and will continue to be geographically dependent when a firm operates in multiple jurisdictions. This is why many solutions will not appear as having wide-spread adoption but will still perform well in areas requiring specific innovation. What is relevant in one jurisdiction (or industry) may not translate to another. For example, the U.S., U.K., and other European countries more widely accept adoption of AI tools like TAR to assist with litigation than jurisdictions in other parts of the world lacking legal technology sophistication.

When looking at technology and globalization, market potential has evolved because firms do not need to operate

in-country to obtain international business since remote capabilities are more prevalent than ever before. While the law firm that does have offices in a certain country will already have resources in place and be familiar with the jurisdiction's technology preferences, one that encounters a global matter as outside counsel will need assistance to leverage the right tools and processes. This is where emerging technologies become pivotal in creating global processes, delivering collaboration capabilities, remaining competitive in global markets, and achieving operational goals.

Transformational Solutions and Processes

Creating a business transformation initiative can help law firms drive impactful operational change and cost savings while addressing global gaps. When setting goals, consider which resources to leverage that carry a track-record of success. For example, traditional front-end office and administrative operations now can be completed virtually if desired. Centralizing operations even when a firm has locations in several countries is extremely beneficial from a cost, time management, and staffing perspective. Some models even offer 24/7 support 365 days a year through the use of captive centers, which is a compelling feature when workflows expand across borders. Having around-the-clock support alleviates worries about projects not being completed on time and maintains the firm's operational capabilities regardless of physical office location.

Business transformation also applies to strategy-driven functions such as creating global workflows or document repositories as a part of an information governance program or effectuating cross-border document review and data transfers to meet litigation goals. Look for a provider operating centers of excellence in locations that are strategically appealing to the firm's needs. Say a firm is in the U.S. but received a new line of business requiring significant document processing or hosting activities in Asia. An effective solution would be to outsource these functions to a center located in the country relevant to the project that offers global 24/7 expert support. Altering processes in this manner allows the firm to meet deadlines, maintain compliance, manage costs, and advance legal defensibility.

Remember that virtualizing assistance and support for international teams can be helpful as a full-time resource or on a project basis, depending on the firm's global presence (or lack thereof). For example, firms with offices in several countries will likely have lawyers regularly collaborating on cases or other projects together. Virtual assistants, project managers, or call centers may be an optimal solution to address consistent needs. The goal would be to configure internal spaces in a manner that consistently promotes and fosters global collaboration. Today, firms without a physical global presence often encounter cross-border matters requiring expertise or processes outside their operational norms. This is where contracting for providers with expertise or language capabilities in that area would be optimal. At times, global litigation will require in-country eDiscovery review. Providers with a physical data center or flex attorneys in that region are valuable resources to meet that need. Even without review mandates, conducting review remotely or in other countries will help firms reduce costs while still obtaining quality work product within relevant timelines. As noted, processing and hosting can also be accomplished at many of these global centers, so bundling these services can even further streamline task completion and create cost predictability.

As mentioned, firms can collaborate with a trusted provider that supports and guides transformation efforts while prioritizing global needs. Consultation and planning to target which areas require enhancement will drive meaningful change. Look for expertise and innovative technologies that align with the firm's global business requirements. Flexibility is key to help standardize workflows while allowing room to adapt for requirements imposed by specific regional locations and to adjust scale. Enlisting assistance will accelerate global business transformation while also providing domestic benefits, which helps streamline everyday operations and reach fruitful case resolutions more expeditiously.

To learn more about Epiq's Business Transformation Services, click here.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Fostering Safe Cloud Integration into Business Operations with these Security Basics

The cloud intersects with personal and professional worlds for many people. Want to share photos with family from a recent trip? Upload them to a shared cloud drive and text out the link for access. Need to have several hands on a project that is subject to a strict deadline? Create a collaborative document stored in the cloud that updates in real time so users can view and edit instantaneously. In the digital age, people want everything available immediately. This need aligns perfectly with the cloud's features, which means the technology will only continue to trend.

This is especially true looking from a business perspective, as organizations in most industries have gone remote to some degree or deploy global operations. As with any operational process or tool, security should be a top concern. But how can organizations sufficiently secure the cloud – especially when sensitive company data backups are maintained in a public cloud network subject to third-party controls? Here are some basic cloud features and security tips that will go a long way and create a solid foundation when the time for added protective measures arises.

Private vs. Public Cloud

Put simply, the difference between private and public cloud rests on infrastructure. Private cloud is akin to a data center and will use an organization's internal infrastructure. In most situations, the organization owns the private cloud. A public cloud operates off a shared infrastructure and has an outside host provider. The organization will pay a subscription fee and will not need to expend a large chunk of money to set up the network internally, unlike a private cloud model. Some organizations take a hybrid approach and integrate both private and public clouds into operations. Regardless of which model is chosen, organizations need to maintain proper security controls to protect their data and remain compliant with all legal, regulatory, and contractual obligations.

Security Best Practices

With the overwhelming amount of data breaches emerging in recent years, organizations must ensure there are adequate

physical and cyber security controls in every setting involving data. Security considerations for the private and public cloud will differ in several regards. When creating a private cloud network, the organization will be solely responsible for managing all security efforts whether done internally or outsourced. Best practices include firewall protections, physical security measures, multi-factor authentication, and added internal controls. Even if not outsourced completely, consulting with experts familiar with private cloud infrastructures helps guarantee protection is sufficient and updated when necessary.

Securing the public cloud is a frontier many organizations have not yet conquered or even believe to be necessary because it involves a third party tasked with security responsibilities. Although true, it is still crucial for organizations to ensure that the cloud provider is deploying sufficient protective measures and independently enhance security in the public cloud. More controls may be needed simply depending on the nature of data an organization is storing to keep hackers at bay, such as sensitive data subject to regulations that require higher measures to keep compliant. Additionally, many agreements incorporate shared responsibility dictating physical security controls to the provider and other obligations to the subscriber (like encryption or authentication). Here are three security basics that will guide organizations on their journey of securing a public cloud:

1. **Shared responsibility:** It is crucial that subscribers understand their role in the shared responsibility model, which is the foundation of public cloud security. This is an area many do not consider because they believe their information is secure simply because the provider will deploy security measures over data in the cloud. However, provider security only represents a portion of the needed security and leaving this gap unfilled will significantly increase breach risk. Cloud providers will generally give their customers a diagram delineating security responsibilities. Basically, the provider only owns the security of the cloud, including infrastructure and network. However, the subscriber is responsible for security in their cloud environment. What is needed will depend on the individual services selected and configurations deployed, such as a specific storage solution.

2. **Provider preference:** Cloud service providers have a vested interest in maintaining security over the data guarded on their platforms and want to ensure their subscribers deploy sufficient controls to limit exposure. As such, many providers will create security recommendations that subscribers should make an effort to understand and match. While this can be very technical, begin with simpler endeavors like identity, access management, login capabilities, encryption, and data storage controls. Understanding these basic security mechanisms and aligning with provider preferences will help organizations better identify future gaps that will require tool augmentation and increased investment.

3. **Asset management:** Understanding the data an organization currently has in the cloud is crucial to define appropriate security needs. Necessary steps include inventory of cloud resources (data and services), consideration of team silos, reference to industry framework, and risk evaluation. Also determine any compliance obligations certain data invokes that would indicate the need for stronger security. This includes regulatory, legal, and contractual requirements. Remember that asset management is a continuous process as new and existing data flows into the cloud. Depending on storage or security needs, an organization may need to utilize more than one public cloud.

4. **Identity authentication:** Gaining access to login credentials or failure to require identity authentication is the easiest way for hackers to get into the cloud. Too many breaches result from stolen, leaked, or improperly configured credentials. Organizations can prevent this by encrypting login data, adding additional authentication measures, managing and monitoring user identities, instituting alerts for failed access attempts, and utilizing trusted technology to ensure these measures are effective.

These basic security steps create a solid foundation to build upon and will limit the risk of highly preventable breaches. Consulting with the cloud provider and security experts on more complicated measures will help organizations meet their shared security responsibilities, maintain relevant compliance, and properly safeguard their data in the public cloud.

Conclusion

Cloud security is a new concept for many organizations. However, there needs to be widespread adoption across industries to promote good security habits and keep company, client, and consumer data safe. Incorporating security into quality process is crucial for cloud providers and an organization's security team. The baseline considerations discussed above supplies the tools to create a confident foundation of cloud security that limits breach potential. Remember that cloud technology is dynamic which means that security needs will shift or evolve, so auditing is crucial to maintain proper data protection.

For more information, consider listening to the corresponding Cyberside Chats podcast.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

New Sedona Commentary Tells Us Protecting Privilege Can be Easy with Rule 502(d) Orders

During the early phases of a case, there are times where disclosure of privileged information may occur. Although lawyers should do everything to protect confidential client information, communications, and work-product documents, mistakes do happen especially during initial investigation and pretrial discovery where the scope or direction of the case is unclear. So, what does this mean when a party wants to claw back privilege over information that was disclosed earlier? Enter Federal Rule of Evidence 502. Under subsection (d), a party can proactively request a court order that prevents waiver of privilege when disclosure occurs. This protection applies to the current litigation and any other state or federal proceeding, even when different parties are involved. Consent from opposing counsel is not required and a judge can also unilaterally enter a 502(d) order.

While it seems obvious that this order would provide many protections, many parties have not been requesting them. Last August, the Sedona Conference released a commentary that is forthcoming this year providing reasons why 502(d) orders should be standard practice in federal proceedings. Here are a few key observations that Sedona made about this topic.

Rule 502(b) is a burdensome alternative

Sedona's commentary attributed slow adoption of Rule 502(d) orders to lack of understanding not only about the protections such an order can give, but the fundamental difference from Rule 502(b). The test under Rule 502(b) applies when there is no prior entry of a privilege disclosure order. To avoid waiver, the party asserting privilege must prove that the information disclosure was done inadvertently, they took reasonable steps to prevent disclosure, and afterwards they took reasonable steps to correct the error. This places high evidentiary responsibilities that can be difficult to prove and the decisions ultimately lack uniformity.

Extra costs, delay, and privilege waiver can result from defaulting to the Rule 502(b) evidentiary test. To remove these risks and ensure protection over sensitive client information, parties simply need to request a privilege protective order.

Lawyers can create standardized Rule 502(d) orders

The advantages of entering a Rule 502(d) order include streamlining both privilege review and the entire case, better cost control, less waste of judicial resources on privilege motions, the ability to determine the level of privilege review necessary for each case, certainty over what communications and documents will be protected, and reduced risk of legal malpractice assertions. To remain ethical, Sedona warned that it is important for lawyers to discuss with their clients the benefits and risks of producing documents after performing a limited review and gain approval before proceeding.

The commentary noted that these orders do not need to be overly detailed, but should include the following components:

1. Producing documents or communications protected by attorney-client privilege or the work-product doctrine, inadvertently or otherwise, does not constitute a waiver.
2. The order applies to both hard copy documents and ESI.
3. The order applies to the case at hand as well as any future federal or state proceedings.
4. The order does not limit a party's right to perform a relevance/responsiveness review when they segregate information or communications protected by attorney-client privilege or the work-product doctrine prior to producing responsive documents.

Limiting an order to inadvertent disclosures could cause issues, as Rule 502(d) does not provide this restriction and doing so could invoke the Rule 502(b) test, which would defeat the purpose of entering such an order in the first place. Additionally, Sedona noted that they add in the inapplicability of Rule 502(b) as an abundance of caution because a minority of courts have ruled such disclaimer is necessary.

Parties should account for unique circumstances

While the above factors provide privilege protection, parties can always add additional terms. As such, it is important to ponder any potential challenges and decide whether extra provisions would be helpful to limit disputes and streamline the case. Consider further researching the following:

1. Placing a cap on the volume of documents a party can claw back
2. A timeframe to assert the order's application
3. Specifically mentioning depositions or evidence inspections, such as the distinction between when the evidence is used versus disclosed and in what situations the order remains effective

Carefully considering potential implications will help lawyers make an informed decision about incorporating unique provisions into a Rule 502(d) order. Future case law or amendments may address unique events like depositions and other ambiguities, so litigators should monitor new developments and implement necessary changes when drafting subsequent orders. It is also a good time to start incorporating these orders into litigation readiness plans and discussing potential benefits with clients. With Sedona's firm stance and thorough analysis, more litigators may be better informed and decide to jump on the Rule 502(d) bandwagon.

If you enjoyed this blog, consider reading Sedona Commentary Provides Ephemeral Messaging Usage Guidelines

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Pandemic Bankruptcy Battles: Looking Back and Beyond

Over the past two years, the number of bankruptcies filed has fluctuated due mostly to circumstances created by the pandemic. Organizations across every industry were not prepared for such a crisis and scrambled to lessen the financial fallout. Industries hit the hardest at the start of the pandemic included retail, entertainment, travel, hospitality, restaurants, and energy. While there are still many unknowns going forward, businesses are trying their best to recover. However, most government aid has ceased or is winding down, and rising inflation and tightening monetary policies will threaten some companies' ability to remain financially strong. This allows for more realistic 2022 predictions – and what is likely on the horizon is an increase in bankruptcy filings.

2020 and 2021 Bankruptcy Review

During this chaotic and uncertain time, organizations in all industries had to reconfigure operations to adapt as best they could. Individuals across the world changed patterns, including how often they left their home, how to spend money, and employment paths. The global economic downturn commenced. This situation coupled with government stimulus caused some unusual bankruptcy activity. Here is a recap of major bankruptcy trends seen throughout the pandemic:

- In 2020, there was a 40% increase in commercial filings. Mandatory shutdowns beginning in March 2020, adversely affected many businesses as they experienced a sudden drop in demand for their products and services. Three industries hit hard were retail, energy, and restaurants. Bankruptcy filings especially soared during the second and third quarters as many businesses could not survive the effects of the pandemic. *
- Many predicted that commercial bankruptcy filings would remain high in 2021, however, that was not the case. Economic conditions began to improve in early 2021 due to a number of events including the widespread introduction of vaccines, fewer restrictions on businesses and customers, lower unemployment rates, historically low interest rates, and more government aid dispersed. The result was a record low year for commercial bankruptcy filings, according to statistics gathered by Epiq, which decreased by 50% from the prior year. While some challenged organizations took a wait-and-see approach and hoped that government aid would extend, others avoided bankruptcy by revamping operations to keep their business afloat. For example, many retail and dining establishments enhanced their online presence or created curbside and contactless options.
- Most of the commercial bankruptcy filings in 2021 were low and middle market companies, as the Chapter 11 Sub Chapter V small business statistics gathered by Epiq confirm. There were very few mega or large Chapter 11 cases filed in 2021. With access to a robust capital market and readily available financing, large organizations were able to amend and extend maturities on their loans. One exception was the Chapter 11 filing of Nordic Aviation, a regional aircraft lessor. A December filing allowed Nordic to restructure $6.3 billion in debt.

2022 Bankruptcy Predictions

There are still many unknowns as the pandemic continues, but overall, people are getting back to work and looking at the realities of the economy's slow recovery. Organizations that lost aid or were holding off to see how things would pan out now need to make tough financial decisions. For many, restructuring could be the best solution to continue successful operations or avoid crippling losses. Here are some 2022 predictions that feed off the pandemic bankruptcy trends seen thus far:

- The economy will recover slowly and in waves. Organizations operating in industries where the articulated risk factors for bankruptcy are higher will see the most filings this year and in the near future, until the pandemic's effects subside and economic conditions improve. These risk factors include labor shortages, supply chain disruptions, interest rate hikes, pricing inflation, and lack of virtual offerings. Surges of potential coronavirus variants can also increase bankruptcy risk for those operating off models involving physical presence, as many in the entertainment and travel sectors have been hanging by a thread. Taking all these factors into account, the industries most vulnerable to bankruptcy hikes include retail, hospitality, and travel.
- Healthcare has been a crucial industry during the pandemic, as there has been an acute need for hospitals and other medical facilities to remain afloat during emergent conditions. Healthcare bankruptcies were relatively low in 2021, with only 13 filings among companies with debt of more than $10 million. One of the largest filings in 2021 was Golf Coast Health Care, LLC that operates 28 skilled nursing and assisted nursing facilities in Florida, Georgia, and Mississippi. The industry was, however, experiencing financial pressures pre-pandemic and hospital and healthcare system revenue have declined sharply because of the COVID 19 pandemic. Hospitals have postponed elective surgeries, and many have put off screenings, as well as primary and other specialty care visits. At the same time, the cost of acquiring PPE and other equipment has sharply increased. Those organizations that have been able to put off a restructuring might need to explore bankruptcy options this year.
- Some analysts believe there is a student loan bubble about to burst. Federal student loan payments were recently deferred again until May, and it is unclear whether there will be another extension or payments will resume at some point this year. If there is no further extension, a fair prediction is that the bubble bursting theory may become reality. Inflation, along with other individual debts becoming due, will make it harder for many to make these payments in the same way they could pre-pandemic.

This is the year for organizations to take a hard look at their financial state and create a viable plan. Bankruptcy can be a useful tool to reorganize debt and strengthen operations to achieve a better path to profitability.

If you enjoyed this, consider reading The Future of Student Loans and Bankruptcy – Is There a Bubble Waiting to Burst?

Note: Statistical commercial bankruptcy filing information shared is provided by Epiq Bankruptcy Analytics.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Disclosure Pilot Scheme Updates: What Practitioners in England and Wales Must Know

It has been three years since the disclosure pilot scheme for business and property cases emerged in England and Wales. After several rounds of feedback from practitioners, updates have been made to certain disclosure practices. These changes further align with the program's purpose of promoting proportionality and streamlining disclosure relevant to a case's unique features. While this was only supposed to be a two-year program, it has been extended through Dec. 31, 2022. This provides opportunity for practices to become even more efficient via additional feedback and case law so when the program ends, the disclosure process will remain transformed.

Pilot Basics

This mandatory two-phase pilot focuses on collaboration and only disclosing documents relevant to the issues that advance fact-finding efforts. In most instances, there will be initial disclosure of key documents along with the statement of the case. After pleadings, the extended phase of disclosure ensues and is dictated by five models covering various scope limitations for each issue. The parties outline case issues and appropriate models in a disclosure review document. The five models are:

- **Model A:** Known adverse documents
- **Model B:** Limited disclosure
- **Model C:** Disclosure of particular documents or narrow classes of documents (recently changed from request-led search-based disclosure)
- **Model D:** Narrow search-based disclosure
- **Model E:** Wide search-based disclosure

Parties need to disclose all known adverse documents within 60 days of the first case management where no extended disclosure will commence. There is also a continuing duty to disclose known adverse documents as they come into a party's awareness for all cases. Often referred to as a living pilot, practitioners should continue to watch the evolution of the program and offer relevant feedback about where gaps still exist.

Recent Updates

In November 2021, the Disclosure Working Group (DWG) amended the pilot to address some challenges that have arisen in practice. Below is an overview of what has changed and recommendations on how the legal community should respond.

- A more simplified disclosure process is now in place for less complex claims, with the presumption that claims under €500,000 will generally fall into this category. This threshold is not absolute and claims of any value can be considered to hold lower complexity if the circumstances indicate this. Additionally, lower value claims will not automatically be labeled as less complex if the circumstances indicate they will require more attention. This change was meant to address the disproportionate amount of money and time spent on lower value cases, which did not harmonize with the pilot's major goal of decreasing disclosure costs.
- Issues for disclosure are not the same as trial issues. They need to be concise and limited, with a maximum of five issues for less complex claims. There was also a timeline change meant to further streamline disclosure and avoid wasting unnecessary resources. When the claimant submits a draft issue list, they now must also include proposed disclosure models including a narrowed

definition of documents falling under Model C, when applicable.

After being in practice, a reoccurring issue was disclosure categorized under Model C encroaching into Model D territory. This was the reason for amending the original language and the hope is that practitioners will avoid excess disclosure by providing proposals under Model C that are concise and limited and scope. The new language also provides the ability to propose disclosure definitions for their own Model C disclosure and for opposing counsel, which was not a possibility under the previous language. Where parties cannot clearly identify specific document categories, they must rely upon Model D because it will provide better results.

There is an express understanding that multi-party cases will be more complex and likely require more steps than included in the pilot. Judges should be proactively involved in tailoring disclosure requirements to the case needs and managing the case. Ponder beforehand which party should receive certain documents, as production to all parties will not always be necessary and create disproportionate review burdens. This will limit waste of judicial resources and streamline the review process.

Disclosure guidance hearings were not being utilized often and being dragged on when parties did request such hearing. Now, parties can independently solicit guidance from the court via correspondence without a formal hearing. Courts can offer nonbinding decisions via this method but also have the discretion to hold guidance hearings if needed.

Practitioners will need to alter established workflows influenced by these updates. Best practices for all attorneys handling cases subject to the pilot are a review of these and future amendments, internal discussion regarding amendment implications, training, necessary tweaks to policies or procedures, resources for answering questions, and regular audits to ensure compliance. Since this program is highly dependent on practitioner feedback, consider submitting concerns or illustrations of deficient program components to the DWG to better refine the program.

Key Case Law

Several court decisions have illuminated areas of the pilot needing improvement or clarification since its inception three years ago. Bringing disputes before the court also gives practitioners a channel for providing feedback and allows for focus on the issues that matter most. For example, here are two decisions that have influenced changes to the pilot and provided basis for the program's extension.

- **Castle Water Ltd v Thames Water Utilities Ltd [2020] EWHC 1374 (TCC):** This decision made clear that when dealing with disclosure of adverse documents, parties need to make reasonable and proportionate checks to determine whether any exist and then make reasonable efforts to locate these documents. This duty does not imply that a full-blown search be conducted – just that the parties check with key custodians relevant to the case events. Unless the proceedings change materially, there is no obligation to perform continuing document checks. However, keep in mind that if a party obtains knowledge of an adverse document some other way during the tenure of the case, it must be disclosed.
- **Willow Sports Ltd v SportsLocker24.com Ltd and another [2021] EWHC 2524 (Ch):** This decision was interesting because it dealt with the interplay between pre-action disclosure and the pilot's parameters. The court denied this request because it was too broad and would basically operate as a fishing expedition for the party to gain intel on how to shape their case via which cause of actions to choose. Because the parties were not cooperating, the court noted that disputes surrounding the order would ensue which would waste valuable time and resources. This decision provides notice to parties that such requests will likely be denied unless limited and that counsel cooperation will add to the likelihood of a judge authorizing pre-action disclosure.

While more decisions have unfolded, looking at a snapshot of cases illuminates the reality that with pilot programs gaps will exist and courts play a pivotal role in making directives more understandable and efficient. Overall, the trends seeming to unfold focus on clarifying ambiguous language regarding disclosure operations and a continued focus on party cooperation to improve efficiency throughout the entire process. One area not yet addressed by the courts is the use of use of Technology Assisted Review (TAR), which is highly encouraged by the program. While many practitioners are using these solutions, what is lacking is further evaluation of when TAR procedures are appropriate and adequate. With the new focus on less complex claims, decisions involving TAR usage in this context may appear and would be very instructive. Practitioners must continue to monitor how courts handle new or repeating conflicts throughout the lifecycle of the pilot, how the DWG responds via future amendments, and whether the pilot is extended again to further refine disclosure processes.

For more information on how Epiq can help you, click here.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

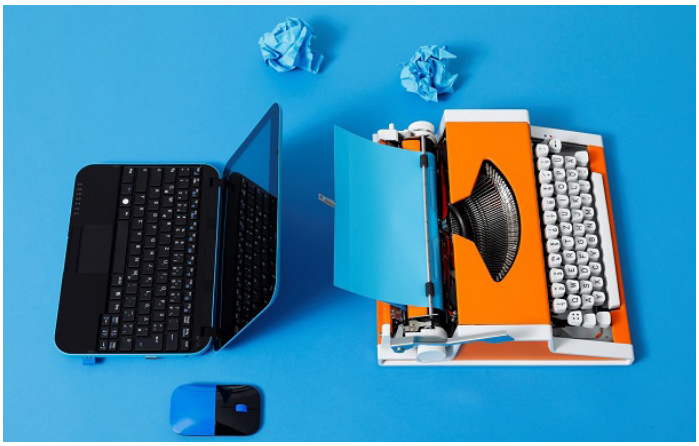
How Can Legal Ops Teams Change Their Tech Approach?

The role of legal operations is increasingly significant in the era of modern law. More legal departments are clearly defining what legal operations encompasses and designating specific teams to advise on functions such as technology implementation, legal spend budgeting, and data analytics. Digitization is transforming business models and teams are striving for an optimal mix of tools and processes to boost efficiency. Historically, technology adoption has been more reactive in nature amongst legal operations professionals. However, there has been trending interest in operating off a more proactive and plan-oriented model. This is in alignment with legal transformation initiatives that many organizations are advancing and will strengthen technology strategy. Turning to innovative technology can improve efficiency, reduce risk, finetune strategy, and optimize department spend.

Compelling Legal Ops Statistics

Recent reports released by the Corporate Legal Operations Consortium (CLOC) and Association of Corporate Counsel (ACC) indicate that legal departments are using emerging technologies and there has been growth, but there is still a lot of unchartered territory to explore that can support legal operations goals. Here are some observations made:

- The 2021 CLOC state of the industry report that analyzes technology and innovation in the legal operations space concluded that the rate of technology implementation across all areas was higher than the prior year. Average legal tech spend was $1.2 million, which more than doubled in a year.
- Participants of the CLOC survey reported that the top technologies their legal departments utilized were e-signature (87 percent); e-billing and matter management (79 percent); contract management (74 percent); and document management (67 percent). Some lower tools on the list were legal analytics, metrics, and dashboards (56 percent); eDiscovery and records management (47 percent); vendor on-boarding and compliance (29 percent); and data science, including AI solutions (22 percent).



- CLOC also reported that automating legal process and implementing new technologies were high priorities for over 50 percent of respondents.
- In the 2021 ACC eDiscovery technology report, 57 percent deemed legal hold software as one of the most effective technologies utilized. However, on average only 35 percent were using legal hold technologies. This percentage jumped to 63 percent when only looking at larger organizations. Turning to a more innovative solution, only four percent of those surveyed had adopted early case assessment tools.
- The ACC identified a trend of more technology presence in mature departments with optimized processes. Almost all organizations at this level (90 percent) deemed technology as a must have and 63 percent planned on investing more into legal software the following year.
- Lastly, the ACC found that most respondents desired a more streamlined experience. Two main problems identified were unconnected applications and struggles associated with learning and using multiple interfaces.

These statistics suggest that while tech reliance has evolved, many advanced solutions with transformative capabilities are being under-utilized. Accelerated change in this space could help legal departments bridge gaps and refine processes.

Fostering Change Effectively

Now is the time for legal operations teams to dig deeper into technology trends and department performance to determine what tools cultivate efficiency. Teams should consider the following when formulating legal tech recommendations:

- **Creating legal tech roadmaps:** Mapping out the department's current processes will shine light on which technologies are working and where underperformance resides. Legal tech roadmaps provide insight into which areas of inefficiency the team should address first and how emerging technologies can build upon or transform existing workflows. A provider with legal operations expertise can consult and help create these roadmaps to ensure tech recommendations or process changes align with department goals and transformation initiatives. It is crucial to identify and manage the best combination of resources, processes, and technologies to reduce overall legal cost while minimizing risk and increasing value.
- **Forward-thinking investment strategies:** Evaluating inefficient operations and diving deep into data can help teams be more proactive with technology. Reviewing ROI and performance metrics on a quarterly basis is best practice. Oftentimes legal operations teams are supporting a large number of attorneys, so investing in tools that can unify workflows on a larger scale is key. For example, implementing a legal intake workflow solution not only enhances efficiency, but also generates data about the nature of legal service requests and FAQs, which in turn informs knowledge management strategies and points to areas where more automation is needed.

Other plan-oriented ways to use technology are data analytics that inform strategy and help set pricing models, solutions that analyze legal spend or can help reduce outside counsel spend, and AI tools for early case assessments to determine which matters are better suited for settlement. These strategic tools limit resource waste, bolster risk management, and provide cost savings. Running a business case analysis can illustrate the long-term benefits of legal tech investments such as these to the department. While certain technologies have associated upfront costs and training, there will be valuable long-term savings and efficiency enhancement. For example, presenting a benefit model as part of a business case for implementing a new e-billing system would ideally include a detailed breakdown of hard dollar savings (eliminating billing errors), soft dollar savings (reduction of manual processes), and potential savings (access to better data that will inform future buying decisions).

By approaching technology with a more proactive mindset and accounting for needs unique to the department, legal operations teams can determine which solutions are the best and begin implementing change more effectively. Modernizing processes and providing tech training will ensure tools are used appropriately and foster growth.

For more information on how Epiq can help you, click here.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Legalweek 2022 Insights: The Great Reflection

Handshakes and hugs between colleagues and friends filled the halls at the annual Legalweek conference held in New York City last week. The thrill of being back in person created an atmosphere of excitement, optimism, and a view to the future while reflecting on the past. Attendees listened to compelling discussions on the state of the industry, attended the keynotes and specialized sessions, learned about innovative solutions while walking through the exhibit hall, and caught up with friends and colleagues they may have not seen in years – or even met in person yet! The conference kicked off highlighting how the pandemic showed everyone that necessity truly is the mother of invention – which brought legal on board what is considered the fourth industrial revolution.

With so much accelerated change the over the last two years, the overarching theme that emerged throughout the week centered on dissecting the past to determine what has worked and what has fallen short to drive future strategic moves and prioritize initiatives. Advancing significant and sustainable changes requires focus on which people, processes, and technologies are best suited to promote future growth. Factors to consider are attainability, budget, and efficiency gaps. Here are some key takeaways explored during Legalweek that aid this journey:

Using technology to create efficiencies and cost savings

A major focus has been on how to do more with the same. This requires a combination of tools that are operationally efficient and customizable with the right people to implement the technologies and help obtain buy-in by demonstrating value. The road ahead holds a greater demand for legal tech expertise. During the state of the industry session, speakers shared that roughly $2 billion was raised for legal tech in 2021. This will drive up demand and foster better tools to use on transformation journeys. Organizations that previously added legal tech into their budget if there was wiggle room are now prioritizing it and carving it out as a separate category of legal spend.

Corporate legal departments are receiving more responsibilities without additional budget, which makes building a sound legal tech stack crucial to aid with a range of varied tasks and initiatives. This includes compliance, DEI, legal spend, and much more. To foster efficiency while still remaining within budget constraints, leverage in-house capabilities in new ways or turn to outside providers that can think outside the box and formulate creative solutions. For example, it may be possible to use past success and process with certain case types to create AI models that will provide a significant jumpstart for similar matters.

Using technology to retain employees and keep them happy

Given the ongoing talent war, people need confidence that their organizations are investing in optimal technology and using it to support other initiatives. Although important and necessary, this goes beyond making flexible work models available or having remote collaboration capabilities. Legal professionals are also valuing organizations that repurpose or analyze their data to inform things like DEI gaps or illuminate ways to drive more purposeful work and cultivate better mental health within the workplace.

Using technology to create a safe environment for data

Cybersecurity concerns will continue to emerge as new data sources are leveraged, regulatory scope increases, and geopolitical matters unfold. It is safe to say that most have accepted the "not if, but when" adage in relation to data compromises. While more organizations are aware of their cyber and privacy requirements, several have not made it up the maturity curve to meet these obligations.

Several speakers at the conference stressed that current cybersecurity responsibilities extend beyond the previous norms of secure perimeters, corporate policies, and up-to-date anti-virus software. They now include information governance, on-going data classification, privacy, insider monitoring, data loss prevention, incident response teams, and more.

Reducing your data footprint by only keeping the data a business needs and classifying and protecting it will reduce your business risk during a breach. This can be achieved by creating information governance policies, audit/certification scope requirements, and privacy controls to help reduce the scope of data to be protected as well as access to that data. Determining what to keep and what to discard invokes balancing of business need, risk appetite, and regulatory requirements.

Should a breach occur, leveraging current technologies such as eDiscovery tools enable organizations to quickly pinpoint sensitive information requiring review and notification so they can meet regulatory requirements.

Another trend surfacing that aligns with "not if, but when," is increased proactivity for cyber incident response. Speakers noted seeing more organizations creating internal cyber breach response roles, consulting with experts in this space, and holding tabletop exercises to foster preparedness for when an incident occurs.

Using technology to transform

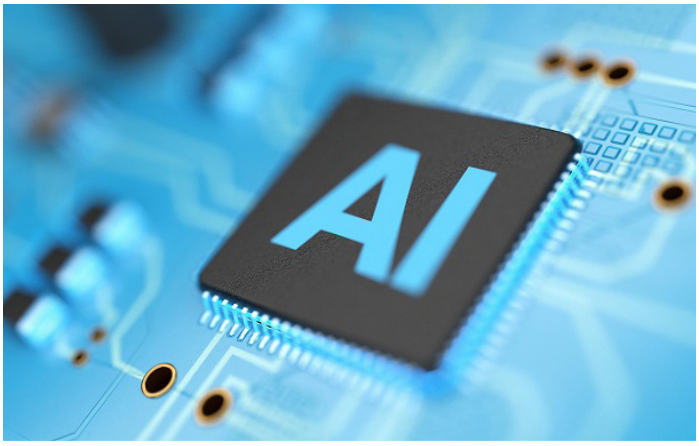
Digital transformation continues to be a large focus for legal departments, firms, and their clients. While using technology in the ways discussed above will definitely elevate transformation, the opportunities to become more efficient and cost-effective are endless. Be intentional with legal tech investments and partnerships by benchmarking, analyzing legal spend, and identifying gaps in existing capabilities and processes. Then, tap into the people and solutions that can unpack value in data insights and effectuate meaningful, sustainable change. Roads to ponder are creating new use cases for eDiscovery solutions the organization already has, such as for incident response efforts or even business purposes outside of legal like tax issues; approaching legal tech roadmaps as living documents to keep informed of legal tech maturity; tapping into data from contract tools to provide actionable metrics that inform subsequent business decisions – including compliance and being able to instantaneously discover how the team handled a similar contract dispute; and layering tools for a case or investigation to obtain better results.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Artificial Intelligence: Using Advanced Analytics to Detect Conduct and Patterns of Behavior

Artificial intelligence (AI) adoption has been largely accepted in the legal community, as many have realized the value of technology that can detect relevant content and produce better outcomes. Incorporating AI into document review workflows or using insights to inform case strategy is transformative and drives better results. From government requests to civil litigation and internal investigations, high profile and fast-moving matters require efficient processes. Deploying technology strategically will help teams to identity key documents and themes early in the case and manage the assessment and review of data efficiently. The continued evolution of AI tools, such as the ability to detect conduct and behavior through sentiment analysis and pattern processing, will further assist with investigatory compliance but can also be used proactively.



Growing Acceptance of AI in the Legal Community

There was a time when skepticism clouded the potential value of predictive models emerging over the eDiscovery horizon. Lawyers were quick to refute the possibility that machine learning and classification of documents could potentially offer a defensible solution to increasing discovery volumes. In a field characteristically resistant to change, this was expected. Despite widespread adversity, advocates such as Maura Grossman and Judge Andrew Peck noted the success of predictive modeling and, as thought leaders in the eDiscovery space, initiated gradual acceptance. The analytics naysayers now appear to represent the minority and the use of predictive models is widespread in Technology Assisted Review.

Yet even during the early days of evolution, when the legal community was just starting to become familiar with TAR protocols and analytics tools, the use of predictive models was already expanding. Advanced investigatory features such as pattern processing and sentiment analysis were introduced as newcomers to the eDiscovery analytics market despite longevity in the field of data science. As use became more widespread, law firm associates and in-house counsel were often impressed during demos, but seemingly hesitant to embrace the functionality within a live workflow. Clients started asking how to effectively leverage these tools and requested assistance with workflow implementation. Market demand necessitated a process devoted to using these tools and legal technologists rose to the challenge.

Exposure to vast amounts of data, with dramatically different content, enabled well-versed users to synthesize the results of both sentiment analysis and pattern processing and develop applicable use cases. It became evident that text-based communications amidst unstructured data yielded the most valuable results, particularly when used as part of investigations or early case assessment. Since "sentiment analysis tools attempt to automatically label the subjective emotions or viewpoints expressed by text," it follows that email communications would be a target rich data pool for this functionality. See John Nay, Natural Language Processing and Machine Learning for Law and Policy Texts (New York University April 7, 2018). In model form, sentiment analysis can be searched upon by score and incorporated as an element of searching. In doing so, when interrogating data, we have an intelligent way to prioritize the search results of custodian Jane Doe, from year 2015, that hit on search terms X, Y and Z. We can sort those results based on sentiment score. Much to the dismay of discovery attorneys, it is still necessary to set eyes on documents to validate the results (and perhaps perform secondary coding); but in theory, users will uncover the most emotionally charged results at the onset of investigation, as

opposed to after a full linear review. The logic behind this method is also applicable to pattern recognition. For example, if we consider the above-referenced custodial data example again, the most anomalous results can be identified and displayed first. This means that if Jane Doe logged off her computer at 5:00 pm every day during her five-year tenure with A Corp, and then suddenly started sending email communications at midnight for a whole week in January, the analytics tool would likely identify this pattern as an anomaly. This can be a valuable function that produces high value results with a relatively low effort on the part of those investigating.

When used carefully, these features offer powerful techniques to identify unusual behavior, potentially inappropriate conduct and emotional exchanges, which are often tied to the underlying legal issues in internal investigations and litigation. Specific examples of conduct that are ripe for discovery using these tools include cartel activity, such as price-fixing and other anti-competitive behavior, sexual harassment and inappropriate relationships, and collusion and employee misconduct. However, potential use cases should not be limited to these situations.

This blog post is an excerpt from the Chapter titled "Outsourced Document Review: Data Intelligence, Technologist Lawyers, Advocacy Support" by Edward Burke and Allison Dunham, which appears in the Thomson Reuters treatise eDiscovery for Corporate Counsel (2022). Reprinted with permission, © 2022, Thomson Reuters. Ed and Allison are eDiscovery experts at Epiq.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Ten Compelling Features of India's Proposed Data Privacy Law

One more country has jumped on the data privacy reform bandwagon. India is soon expected to enhance restrictions. Protections could extend even further than the EU's General Data Protection Regulation (GDPR). This legislative overhaul has been a five-year long journey, with a 2017 Supreme Court decision kicking it off by concluding that privacy is a fundamental right. Soon thereafter, a privacy bill emerged and has been sitting with India's Parliament for over two years. The joint committee reviewing the bill finally issued a report last December outlining some revisions.

Positioned as one of the largest open internet markets and a major hub for offshore outsourcing projects, a comprehensive India data privacy law has the potential to make a lot of waves and influence privacy landscapes all over the world. Some analysts expected it to pass into law this spring, but recent reports indicate that India may create an entirely new bill. This would address fears that certain provisions would inhibit India's growing startup and tech industries, and also some global concerns. For example, the U.S. has expressed apprehension over how restrictions on cross-border transfers and data localization requirements could compromise safe data travel.

Key Provisions

Whether the current bill passes or a new one takes the stage altering some debated provisions, India is on the verge of drastically changing their data privacy framework in the very near future. Here are some important changes that would stem from passage of the pending bill, as proposed:

- Collection and processing activities applying to personal and non-personal data of Indian residents would fall under the law's purview but be afforded different layers of protection. In addition to organizations located in-country, the law would also apply to data fiduciaries and processors situated outside of India. Notice of use, prior consent, and limitations exist to help balance interests of data subjects and fiduciaries.

- Data fiduciaries have several responsibilities when it comes to handling information. Major duties include creating "privacy by design" models; being transparent with process and algorithm usage; and providing comprehensive notice to data subjects that also contains information about things like retention policies or cross-border transfers.

- The right to data portability would exist even when dealing with trade secrets. Data portability denials are only appropriate when technically unfeasible.

- A data protection authority (DPA) composed of no more than six individuals would be responsible for compliance monitoring and enforcement. The DPA must include the attorney general and a director from both the Indian Institute of Management and Indian Institute of Technology. Some key responsibilities would encompass regulating and limiting personal data usage, creating accountability standards for organizations to follow, fostering trust, and establishing penalties for non-compliance. In addition to the creation of a regulatory body in India, each organization subject to the law would need to appoint data protection officers to help attain compliance.

- When dealing with cross-border transfers, the DPA would need to consult the government before issuing approval for a contract or intra-group scheme. Anything against public or state policy would be denied, which leaves broad discretion up to the government.
- For breaches involving both personal and non-personal data, organizations must provide notification within 72 hours of awareness. The DPA could direct an organization to adopt urgent measures to boost remediation efforts.
- The law would impose data localization requirements, mandating that critical data be processed in India. Sensitive personal data could be transferred to another country, but a copy would need to remain stored in-country. The bill also directs the government to issue a detailed policy on data localization practices.
- The government could create sandbox environments for testing new products, tech, and services. This is meant to help startups incorporate "privacy by design" while still advancing innovation.
- Social media platforms would be viewed as publishers and therefore responsible for hosted content posted by third parties. Designating a media regulatory authority may result to help with this feat.
- The government can set up a testing site for hardware and software present on IoT and digital devices. This would help ensure that manufacturers appropriately secure devices.

Looking Ahead

It is critical to keep informed of any changes that occur if tweaks are made before passage or a new bill emerges. Organizations in India and those located abroad that collect data of Indian residents, process and store non-resident data in offshore facilities located in India or anticipate cross-border transfers involving India all need to monitor what happens with the pending bill closely. Major change may occur in a new bill in areas where domestic and international controversy exists around proposed requirements – data localization, cross-border transfers, startup activity, and social media platforms. However, if the current bill ends up passing as is then interpretation of such provisions would be crucial to understand compliance obligations.

Regardless of when new legislation passes and what revisions ensue, proactivity cultivates success. Organizations may update compliance programs, create new data policies, hold trainings, explore tech solutions that promote privacy by design and provide valuable data insights, compare obligations between privacy laws, and reevaluate business models if the burden associated with offshore activities heightens.

Also note how India's approach to privacy influences moves made by other countries. It is not a coincidence that the EU recently introduced draft legislation that would provide protections to non-personal data, which the GDPR does not currently cover. To avoid interference with expansion of the country's digital economy, a successful law needs to balance this interest with consumer privacy rights and compliance burdens. Just as with other data privacy laws, enforcement will help with this feat and also establish a baseline for what is acceptable and where gaps still exist.

If you found this blog useful, consider reading Privacy Roundup Part Two: Significant International Updates.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

The Changing Landscape of Dawn Raids: Preparing for Hybrid Inspections

The pandemic accelerated widespread digitization in almost every industry. Moving from hard copy to digital documentation influences many business and legal processes, including the way authorities around the world conduct dawn raids. This is an unannounced inspection by regulatory or criminal investigatory authorities into matters such as antitrust law, financial markets regulation, data protection, and financial crime. They typically occur in the morning and have generally been carried out onsite. However, the rise in remote work has altered investigatory approaches and there has been a notable increase in hybrid raids. Teams can simultaneously raid physical offices and private residences to ensure they collect data on remote worker devices – sometimes in multiple countries.

Although dawn raids are not frequent, they occur without warning and can put an organization at significant risk for noncompliance if not prepared. It is important to know who can conduct dawn raids and how investigations are shifting with the remote work culture. This knowledge better positions organizations to proactively create plans limiting risk.

Authorities

The U.S. Department of Justice (DOJ) Antitrust Division has the power to investigate anti-competitive behaviors in both civil and criminal contexts. Dawn raids occur more often in the U.S. for matters involving suspected criminal antitrust violations, such as collusion. DOJ officers, FBI agents, and local law enforcement can enter the premises (offices and local residences) to investigate after obtaining a search warrant.

Hybrid dawn raids are also ramping up in other locations around the world. For example, last year the European Commission announced a wave of post-pandemic dawn raids. The Commission has statutory powers to investigate anti-competitive practices affecting trade between EU member states such as restrictive agreements and abuse of dominance.

Penalties can include fines and imprisonment for criminal matters. Organizations can also receive fines for noncompliance with procedural mandates such as failure to turn over requested documentation or concealing evidence.

Considerations and Preparation

If organizations handle a dawn raid incorrectly, significant liability may result. The trend of increased hybrid raids can be daunting, as many do not have a solid plan that accounts for custodians working remotely. To reduce the shock factor and keep compliant, it is crucial to be prepared and leverage partnerships that will limit exposure and foster preparedness.

Here are four ways to enhance dawn raid preparedness:

1. Understanding risk factors: Knowledge of the type of data an organization maintains will uncover which information is at risk and the regulatory bodies that would control potential investigations. Certain business activities increase dawn raid vulnerability, such as communications between organizations that could appear as collusion or collecting sensitive consumer information invoking data protection legislation. A proactive risk assessment allows for earlier custodian identification, notification, and training opportunities.

2. Mapping data: Many organizations already utilize data mapping as an information governance tool. After determining that an organization could be subject to a dawn raid, specific mapping for high-risk data will aid with investigatory compliance. Mapping should entail identifying, understanding, and plotting what information an organization has, how the data flows through the

organization, who has physical or remote access to the data, and where the information is stored. Mapping can also uncover improper data handling by remote workers that organizations need to address. Establishing control and accessibility allows for easier retrieval and assessment of privilege during a sudden investigation.

3. Forming response teams: The core team should include onsite reception, IT staff, legal counsel, management, human resources, and any outside partner overseeing forensic collection or compliance efforts. Also account for key custodians who could be subject to at-home investigations. Provide proper notice and training on what can happen during a raid – including an active search of the premises, interviews, inquiries about storage locations for relevant documents, and seizure of evidence for review off-premises. Regarding electronic data, investigators can seal off premises to prevent interference with data sources, request passwords, copy drives, remove devices, and more.

   Second, anticipate challenges that could arise and confirm what constitutes acceptable behavior. Some actions to avoid during a raid include hostile reception, evidence destruction or concealment, providing false or misleading information, and access obstruction. Absence of a plan could also lead to leakage of privileged information, so make sure the team has knowledge of what they can withhold.

4. Performing readiness assessments and mock exercises: Evaluating and testing policies and procedures will identify gaps. Consider partnering with a provider with experienced experts offering a combination of regulatory knowledge and forensic IT skills to guide assessments. Having an initial workshop can be beneficial to discuss procedures, common challenges, overcoming obstacles, and best practices for dawn raid preparedness. This also provides opportunities to voice anticipated concerns and uncover rick factors.

   A readiness assessment can be a valuable tool to create a risk matrix, map data, establish a tailored response framework accounting for hybrid inspections, and determine whether to hold a mock dawn raid. All of this will strengthen the foundation of an organization's dawn raid readiness program. Providers can also work in tandem with the team to improve programs and implement best practices leading up to and during a raid. This includes:

- Understanding how to image or copy data on devices
- Creating a memorandum for regulators outlining information management, storage, and retention policies that is regularly updated
- Circulating an internal dawn raid procedure memorandum for both onsite and remote employees
- Copying data seized and imaged by regulators to assess potential exposure
- Observing and noting the entire investigatory process

These are just a few key components of a robust dawn raid readiness program. Regular assessments and audits will highlight specific processes that reduce exposure and streamline compliance in the event of a dawn raid, while also accounting for the likelihood of hybrid raids based on the organization's remote work policies.

For more information on how Epiq can help you, click here.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Three Key Components of a Global eDiscovery Strategy

Global litigation is more common today as international business deals, emerging technologies, and new regulations invoke cross-border obligations. Since many countries have now adopted eDiscovery processes, it is important for legal teams to factor that into their litigation readiness plans and develop dynamic protocols to account for this legal shift. With this comes challenges, as developing international strategies subject to varying and sometimes conflicting legal directives can be time-consuming and costly. Organizations need to contemplate potential obstacles and proactively create resolutions to lessen the risk of progress impediments during a cross-border case. Some have already initiated this process. In a 2021 study, Ari Kaplan Advisors questioned 30 in-house leaders responsible for eDiscovery at larger organizations spanning several industries. Of the professionals interviewed, 60 percent employed a global eDiscovery strategy at their organizations and 67 percent followed eDiscovery protocols worldwide.

Below are some important items to consider when creating a global eDiscovery strategy:

Discovery laws and regulatory influence:

- When dealing with global litigation, each country will almost always have different approaches to eDiscovery as this is now a multinational discipline. This requires knowledge of all laws relevant to a case. For example, China has unique data transfer rules making certain organizations subject to state secret reviews of data before it can move across borders. If information related to a global case is stored in China and subject to extra restrictions, this can significantly impede eDiscovery review. As such, it is important to have established processes to approach and streamline obstacles like this. Additionally, if a country forbids a cross-border data transfer then the legal team needs to have a way to host, process, and review the information in the origin country without blowing their litigation budget. Sometimes it will be necessary to weigh the value of the information to the case against the costs.

From a regulatory compliance standpoint, all legal teams need to be aware of the consumer privacy laws popping up worldwide – especially because many carry an extraterritorial reach. In the eDiscovery survey noted above, 47 percent of participants reported that the EU's General Data Protection Regulation (GDPR) affected their eDiscovery protocols. Privacy compliance should be embedded in litigation plans to account for situations where data access may be challenging or an organization will need to implement extra steps to avoid non-compliance with GDPR or other data privacy laws, as large fines and case delays can result. Some necessary controls to explore include increased data security, local hosting as opposed to transferring data across borders, global eDiscovery training, and data mapping. Also look out for any U.S. court decisions covering discovery needs that conflict with international regulatory obligations, as these will be instructive and critical due to varying privacy landscapes and high potential for data storage outside U.S. borders.

Cost considerations:

- It is important to factor in anticipated and fluctuating costs when creating a global eDiscovery budget. Besides the standard review costs associated with a strictly U.S. case, other potential costs include international data centers,

research, extra staff, multilingual technology solutions, travel, translation, and licensing. Each project's needs will vary but will definitely drive up costs due to unique global requirements, so legal teams will need to factor in some flexibility in their budget. Look for predictable pricing models with customization options to use for more than one matter, as this promotes better cost control.

Partnerships advancing eDiscovery objectives:

- When creating strategy, the team must balance local laws against the desire for uniform processes, suitable technology investments, and execution of global business workflows. Collaborating with a provider that has a global reach and expertise with eDiscovery requirements abroad is cost efficient and provides a consistent defensible approach to international issues. It is important to find a provider with language capabilities or local data centers needed for the case that understand varying legal and regulatory landscapes affecting eDiscovery processes. When hosting and review is needed in another country, such a partnership can reduce significant travel and project assembly costs. Even when most of the discovery work commences in the U.S., it is still necessary to incorporate requirements from other legal systems that play a role in the case into global eDiscovery strategies. Remember to consider data privacy controls to maintain compliance and avoid review roadblocks. For some organizations, a managed services arrangement with a global eDiscovery provider may be the best avenue for cost optimization and risk management.

Remember that global eDiscovery strategies will evolve as legal landscapes around the globe change. New eDiscovery and data laws both in the U.S. and across borders will continue to influence global litigation and present unique challenges for legal teams. The approach needed will also look different depending on the case components and location of key eDiscovery data. Having a structured yet flexible base strategy factoring in the components above and allowing for flexibility will make the process more manageable, lessen risk, address budgeting concerns, and avoid wasting resources.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Where to Next? Travel and Bankruptcy Predictions Remain Foggy

There is no argument that throughout the pandemic, travel has been one of the hardest hit industries. Domestic and international restrictions, capacity limitations, cancelled events, remote operations, illness, and fear caused people to travel less for both business and pleasure. This led to a record-breaking decrease in airline bookings and hotel stays during 2020 and 2021, which brought heavy financial burdens. Whereas restaurants and retail could pivot to an online sales model, airlines and hotels did not have this luxury. Hotels in particular were left with limited to no options for supplementing revenue.

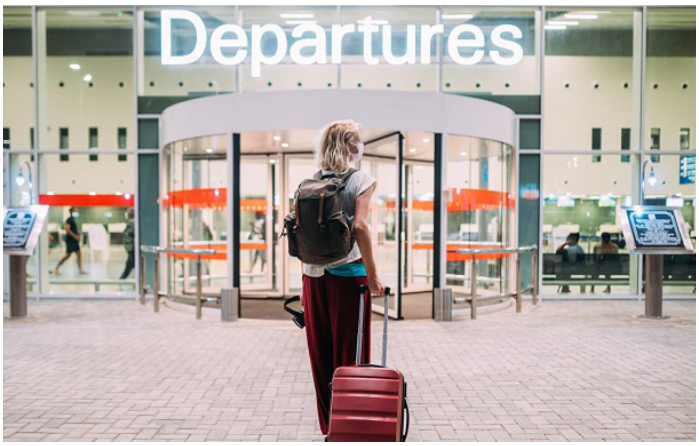
With travel on the rise again, it looks like the industry is starting to rebound but the strain of the pandemic and ongoing uncertainty in the world persists. Due to the continued volatility, organizations should proceed with caution, be mindful of trends, and determine if there is value in developing a restructuring strategy. Below is a recap of what has been happening and thoughts on what is next for the travel industry.

Challenges and Observations

Airlines and hotels suffered immense hardships, but most have been able to continue operating. Here are some major trends that have materialized.

- **Domestic airlines:** For major U.S. airlines, government aid and reliance on alternative revenue streams saved many from bankruptcies. The aid consisted of $54 billion in payroll grants with lower future repayment mandates and taxpayer stock warrants. The government also made $25 billion in low-cost loans available. Now that aid has slowed, we will see if airlines can remain afloat without any major restructuring. Rising fuel costs and continuing supply chain issues as well as general uncertainty related to the ongoing pandemic will likely plague the domestic airline industry for the near future.

Major airlines such as United and American have been able to hedge some losses with cargo revenue, given increased demand for this costlier transportation option due supply chain constraints. Airlines made strategic decisions about how to enhance and prioritize this portion of the business that, in the past, generally was a smaller subset. Boosting cargo business helped supplement profit dips from diminished passenger



travel while also alleviating major supply chain issues and delivering medical supplies or vaccines during these times of crisis.

- **Foreign airlines:** Several foreign airlines have taken shelter in U.S. bankruptcy courts to restructure and sustain future growth due to lack of aid, less access to capital, and low flight volumes. For example, Aeromexico was able to maintain operations by filing for Chapter 11 in 2020 and restructuring assets. The carrier has successfully emerged from bankruptcy valued at roughly $2.5 billion with solid investors and a strong capital structure. A New York holding company that lent the carrier $1 billion will be the largest shareholder and Delta holds 20 percent ownership.

- **Hotels:** Lack of hotel bookings resulted in urgent decisions related to cost minimization. This included downsizing staff and shutting down partial operations such as onsite pools, spas, bars, and restaurants. Hotels catering to specific travel purposes – such as those situated near theme parks or national attractions – suffered even greater losses. Government aid, emergency funds, and loan forgiveness has helped fend off mass bankruptcy filings. However, even as travel rebounds some struggle with lack of staff and inability to reach pre-pandemic occupancy levels. Also, the competition with alternative lodging options such as Airbnb that was already present adds to the strain and market competition.

Predictions

Optimism is returning as vacations, business conferences, concerts, and other events are happening again. However, the lingering uncertainty and damage caused will likely make travel recovery a long, albeit steady haul. Factors contributing to volatility include the potential for more COVID-19 spikes, high fuel prices, union disputes, inability to staff planes due to labor shortages, and continuing supply chain interruptions. Here are five predictions on how the industry will fare going forward:

1. Business travel will have a slower revival due to remote working trends and recent technology advancements. This, coupled with some international travel restrictions, will cause global organizations to be more strategic about the resumption and frequency of in-person meetings and events.

2. Overall, U.S. airlines should fare better than foreign airlines. Planes are filling even with the increase in fuel prices because people have pent-up demand for travel. Major airlines have incorporated creative strategies such as hedging cargo revenue, which helps recoup losses and becomes pivotal in the event of future travel interruptions. However, sustained recovery depends on many variables including a sustained decline in new infection rates, the consumer travel index remining high, and the ability to manage fuel prices and labor costs. If these variables remain unchecked, and there is no additional government aid, it could lead to distress in the industry and some U.S. airlines may need to consider bankruptcy.

3. Foreign airlines have a harder hill to climb with lack of government aid and lower passenger travel, especially on long-haul international flights, so we will likely see more foreign airlines seek relief in U.S. bankruptcy courts or explore other restructuring options.

4. Lenders offered deferment options for many hotels to help alleviate the economic impact and provide a recovery buffer. Although hotel bookings have seen a steady increase since mid-2021, many hotels are still financially stressed. Hotels that cannot retain adequate staffing levels, face union issues, or are not seeing enough bookings to boost revenues have a battle ahead. There is a good chance that lenders will start pursuing debts more aggressively, especially since reporting requirements have resumed. If this occurs, hotel bankruptcies will inevitably rise.

5. A major trend in 2021 across industries was increased prevalence of pre-packaged bankruptcies where the debtor establishes a comprehensive plan before filing for Chapter 11 to streamline the case and minimize costs. This will remain an ideal option for domestic and foreign airlines, as well as travel management companies.

While the travel industry has dealt with economic downturns in the past, it has not experienced these unique circumstances in recent history, and it is difficult to predict what will happen next. Travel is currently in a transitionary period and will recover fully at some point. Some companies will weather the storm and others will struggle under heavy debt burdens and will have to restructure or file bankruptcy.

If you enjoyed this blog, consider reading Pandemic Bankruptcy Battles: Looking Back and Beyond

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Delete Data, Save the Environment

Incorporating data deletion practices into information governance initiatives provides many operational and cost-saving benefits. Retention policies should address what type of data to keep, for how long, and which devices employees can use for business purposes. Factors such as compliance obligations, workflows, and case needs will influence policies. Artificial Intelligence (AI) is a great tool that can be used for data deletion decisions. For example, AI-based reduction for eDiscovery provides legal teams with a more focused data set, saves resources, pinpoints key issues quicker, and streamlines resolutions.

Less data leads to better organization, lower storage costs, fewer documents to review during a case or investigation, freed up resources, and dark data reduction. This also provides valuable environmental benefits that often go overlooked.

Data's Influence on the Environment

Many people do not think about the physical presence data has in our world. While sending emails or texts instead of snail mail cuts down on paper usage, this data still exists somewhere on a physical server requiring energy sources to operate. A ton of unneeded data lives on devices and in cloud storage taking up space and energy. Think about all of the spam or subscription emails sitting in various inboxes. In 2020, Good Planet concluded that the average American has 500 unread emails consuming energy and producing extra carbon dioxide. This is just looking at one data source, and emerging technologies will only increase the amount of data present in the world. With organizations leveraging new tech and operating off hybrid models, it is crucial for those that have committed to prioritizing environmental initiatives to think about how their business practices tie into their overall carbon footprint. Simply put, less data means reduced server space, resulting in decreased energy usage. Being proactive with information governance and AI implementation can advance this goal.

Four Data Reduction Tools

Data deletion and reduction are strategic factors that most organizations consider to some degree. Here are practices to

implement or strengthen that will not only enhance operations and efficiency, but also reduce an organization's carbon footprint.

1. **Retention protocols:** Information governance is an ongoing effort to manage information from multiple perspectives with multiple objectives. There is always room for improvement. Organizations should reevaluate retention policies once a year (if not more frequently) to factor in compliance, stale data, migration needs, duplicative files, and similar concerns. Consider environmental goals as a part of this process to further refine retention processes. For example, look into whether employees are saving the same document or graphic in several locations. Addressing matters like this will declutter internal storage while also lessening the impact that saving multiple copies has on the planet.

2. **Communication controls:** Email and instant messaging are common places where data builds up, thus requiring more physical server storage. Analysts have found that the average office worker receives 121 emails per day, which equates to 0.6 tons of CO_2e a year. Having policies around deletion and subscription allowance for work emails and messaging systems are simple strides that can contribute to less fossil fuel usage resulting from the energy needed to power data storage centers. Automating deletion after a certain timeframe on messaging systems is a good option to explore. Email oversight is a little trickier to automate, as

so much content variety exists in a person's inbox. Training and management check-ins on compliance would be helpful tools in this area.

3. **Early Case Assessment:** Legal teams have been using TAR and similar tools for years during the eDiscovery review phase. A new trend is leveraging AI tools at the outset of a case or investigation to cull datasets and focus review. This eliminates unnecessary data to host, review, and exchange with opposing parties. Legal teams are also able to uncover insights that aid with settlement negotiations, case strategy, and valuation. The downstream effect can help close matters quickly and efficiently while also saving energy. In 2020, Data Center Knowledge reported that data centers use about one percent of all electricity in the world each year. Increased digitization will only make this percentage larger, so any small effort can contribute to making a difference.

4. **Other AI avenues**: There are many innovative AI solutions that can help solve various business challenges while also reducing data. For example, using AI when migrating to the cloud can ensure that only documents designated with business use, under legal hold, or needed for compliance move to the storage platform. Automated tools that can classify data will help determine what to keep and what to toss. Also look for cloud providers that build sustainability into their models when vetting potential partnerships, as the provider's efforts will translate to the organization.

Determining where process gaps exist can also shine light on where organizations can use AI to reduce human error and improve efficiency. Layering tools for a case or investigation will accomplish tasks faster with more precision. Other areas to explore include contract management, contract analysis, and privacy compliance. Simply put, less data to review and human intervention will ultimately save on energy. Building environmental concerns into workflows can also provide opportunities for AI-generated data insights that illustrate whether an organization is meeting goals for reducing its carbon footprint. This provides a basis for auditing, extra training, and changed processes to continuously improve sustainability efforts.

Conclusion

Through the mechanisms above, organizations can reduce their carbon footprint while also transforming business practices, advancing efficiency goals, and meeting compliance obligations. This is a win-win situation with opportunity for growth. Remember that education and oversight are crucial to success and new habit formation throughout the organization. Use data insights to benchmark progress and help effectuate change. Organizations on transformation journeys are likely already advancing these steps, however being aware and building sustainability into planning will only enhance outcomes further.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Rising Premiums and Ransomware: The Cyber Insurance Balancing Act

Threat actors are developing more sophisticated and strategic ways to target sensitive information. Digital footprints and tech usage will only keep expanding, which adds to vulnerability and presents more opportunities for compromises to occur. Recently, ransomware has taken the stage as the malware of choice with the average estimated cost of a ransomware breach coming in at $4.62 million, according to IBM's 2021 Cost of a Data Breach Report. Demands previously in the thousands are now in the millions. With ransomware attacks now trending, cyber risk elevates dramatically as organizations across industries of all sizes can fall victim.

With greater potential for data compromises comes a greater need to explore cyber insurance. The dilemma that ensues is that when attack prevalence rises, it heightens risk for both organizations and insurers. Organizations need coverage to add an extra layer of protection and insurers need to drive up costs to match the cyber landscape. These increased costs are steep – according to an S&P Global Market Intelligence analysis in 2021, premiums for stand-alone cyber policies increased 28.6% in 2020 alone. Some even refuse to extend coverage to ransomware incidents. Add in that cyber threats are dynamic, and it makes rate predictability and risk evaluation a difficult feat.

Before deciding to issue a policy and when calculating rates, insurers are using cyber risk tools to look closer at an organization's security posture. Claims investigations are also more thorough and insurers are tapping into cyber experts when determining to extend coverage. Below are some strategic moves that improve security posture while also making an organization more attractive to underwriters. While the process remains variable, taking these steps increases the potential that an underwriter will offer lower premiums and cover events in a time of higher risk and rising costs.

Remain cyber aware

The cyber threat landscape is always changing, so it is crucial to keep informed on current threats and trends. While ransomware is causing the most challenges currently, it is inevitable that this will change as organizations are better prepared to avoid these threats or limit exposure risk. Even so, threat actors will unfortunately continue to evolve their

capabilities and find more ways to penetrate systems – whether it be a completely new attack method or variations of current ones. Keeping on top of the changing landscape will help organizations improve policies and procedures related to tracking and managing threats and risks. Addressing cyber risks in your supply chain of professional services, maintenance contracts, software, and finished goods plays a role in staying cyber aware. All of this sets the stage for a robust and effective program.

Ensure cyber controls are mature

While it is impossible to achieve perfection and fend off all attacks, organizations can take steps to mitigate risk. Underwriters are looking closely at the controls in place that would prevent an attack or foster rapid remediation and recovery. To bolster cyber and risk management programs, organizations can implement extra security controls:

- Implement multi-factor authentication to provide effective defense against stolen credentials. Using more than a password to authenticate users is important as it adds another layer to protecting user credentials.
- Encrypt sensitive information such as data containing personal identifiers or trade secrets. Restricting access to sensitive folders or servers is also helpful.

- Perform robust backup and recovery with immutable backups and implement policies around data backup, retention, and recovery.
- Conduct regular security testing to evaluate your systems for vulnerabilities requiring mitigation.
- Monitor security ratings through scoring services like BitSight.
- Ensure employees are cyber aware through regular education and training on trending attack methods and what their role and responsibilities are in keeping the organization safe.
- Use automated security scanning software to detect new vulnerabilities, unauthorized changes, and violations of standards to maintain a security baseline.
- Create internal roles or partner with a provider that can evaluate dynamic risk and provide ongoing strategy and guidance on cybersecurity decisions.

Tools and processes like these will lower an organization's risk profile and make it more likely to avoid compromises and implement swift recovery efforts. This lessens the risk that an organization would need to pay a ransom in the event of an attack. Implementing extra controls prior to applying for new coverage or undergoing renewal can lead to better negotiating power for rates.

Bolster incident response preparedness

Having a strong incident response plan that includes a retainer with a data discovery and forensics firm beyond what your security teams have will assist with recovery in the event of data compromise. Limit exposure by proactively designating response team members, outlining communication protocols, determining which technologies would be best to leverage, and conducting mock exercises. This demonstrates to insurers that the organization has taken an active role in anticipating and minimizing threats.

Explore alternate insurance models

As cyber preparedness rises in priority for organizations across industries and the cyber insurance market matures, new ways to evaluate risk and manage policies will emerge. Bi-annually, quarterly, or even monthly premiums are in the realm of possibilities. Insurers may require more frequent audits that can result in discounts for sound security demonstrations. Failure to maintain proper controls or act in accordance with the policy could result in denied coverage or dropped policies.

When choosing an insurer, it is important to know about emerging models and coverage options to determine if risk appetite meets an organization's needs. For example, if an insurer does not extend ransomware coverage or offers lower rates even when an organization illustrates healthy security habits, it may be time to explore alternate coverage. .

Also consider the additional added value many cyber insurance policies can include – incident response assistance, crisis management services, and more – that may be an asset beyond the direct financial benefits. This may make the insurance policy worth keeping despite pricing increases and coverage limitations.

If you enjoyed this blog, consider listening to our CyberSide Chats podcast on the same topic.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Predicted Implications of the EU's Digital Markets Act

On March 24, 2022, the European Parliament and European Council approved the final text of the DMA. The DMA imposes more regulation over core platform services, such as online search engines, marketplaces, and the like. The Commission will designate gatekeeper organizations – which encompasses big tech providers with over 45 million monthly end users and ten thousand business users in the EU, amongst other requirements – for higher regulation.

Formal approval and publishing of the DMA should occur later this year or early next year. After the law goes into force, there will be a grace period before it is actionable so gatekeepers can provide information and become compliant. As such, expect the effective date to be sometime in 2023 or early 2024. In the meantime, the Commission has encouraged organizations to come forward with any questions to foster compliance. While affected organizations absolutely need to start thinking about updating compliance programs, the DMA holds additional implications for eDiscovery practitioners and can heighten security risks.

Key DMA Provisions

The recent agreement on the DMA is a huge stride in the EU's digital strategy. Violations can result in fines up to 20 percent of an organization's total turnover. Here are four major features of the new law:

1. Gatekeepers will need to provide users with choice over browsers, search engines, and virtual assistants. Third-party app stores will also need to be allowed on gatekeeper platforms to offer user choice.

2. Smaller messaging platforms can request interoperability from gatekeepers. What this means is that users will be able to communicate across different apps. The DMA does not address social media platforms, but this will likely be a topic of discussion down the road after seeing how interoperability works with messaging platforms.

3. Users will need to provide consent before a gatekeeper can process or combine personal data across platforms to initiate targeted advertising.

4. Gatekeepers must provide information to the Commission about acquisition plans for smaller core platform services. In the future, the Commission may have the power to temporarily halt acquisitions in this space.

Expected eDiscovery Repercussions

When a new data law passes, it is crucial for eDiscovery practitioners to consider potential effects. If smaller organizations leverage their interoperability rights, data preservation and collection challenges will undoubtedly emerge. This would affect not only EU cases and investigations, but also those originating in other countries dealing with EU custodians. Combining content across platforms can lead to challenges identifying where data lives, extraction roadblocks, and increased data sources requiring more expense and time. Expect innovative technology and processes to emerge over the next few years that address challenges associated with extracting and reviewing messenger content with multiple file types without missing responsive data, as this is a risk resulting from interoperability.

Others have speculated on ways that leveraging the DMA's interoperability power can benefit eDiscovery processes. Examples include streamlined collection for ephemeral messaging content and less chance of evidence spoliation since there will be more locations where data is housed.

Security Concerns

While the DMA states that interoperability requires high security data protection controls, this function inherently poses security challenges. Gatekeepers and smaller platforms that become interoperable would essentially have to agree to use the same encryption techniques and controls that foster functionality while reducing the risk that threat actors can access the messaging content. It may prove difficult to get both parties on the same page with adequate oversight.

State of the DSA and Beyond

The DSA is still in the works, but recently had some movement. This law is similar to the DMA but has more focus on regulating the content platforms host. Several debated provisions exist, such as using dark patterns to obtain data or purchases, elevating privacy protection for minors, and user compensation when infringement occurs. There have been proposals on these and other issues concerning the level of regulation and wording that should appear in the law. This movement, coupled along with the recent DMA passage, will likely propel the final approval of the DSA sometime this year.

Just as the GDPR continues to influence other countries around the world to update privacy frameworks, the EU's expanded digital strategy could jumpstart a new regulatory trend. Other regulators have similar concerns regarding big tech, so interested parties should watch and see how DMA enforcement unfolds, what gaps the DSA will cover, and which country makes the next move in this area.

For more information on how Epiq can help you, click here.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Time to CLOC Back In – the Live Institute Returns

Last week at the 2022 CLOC Global Institute in Las Vegas, you could feel the excitement to finally be back in person. Whether sitting in on breakout sessions, watching demonstrations in the exhibit hall, or chatting in the hallway with peers – there was an overwhelming sense of community. Legal operations continues to grow and position itself as an industry within the legal industry. The role is evolving and dynamic, with different responsibilities in each organization. Connecting legal to an organization's leadership and business units helps drive transformation and escalate the value of legal operations.

Below are five major trends explored at the event:

1. Change management is accelerating: The legal industry remained stagnant for a very long time. Legal has traditionally been viewed as the "department of no" with a risk averse mindset. Digital evolution started with the use of AI tools like TAR for eDiscovery review. Given the rapid acceleration of tech and innovation that has occurred recently, more legal professionals now accept and trust the use of AI to help sort through data. This next phase includes determining how leveraging the right tech and partnerships can allow the legal department to garner valuable insights that inform better business decisions and increase profitability.

   This is where change management comes into play. While a broad term, this generally refers to helping organizations embrace change in a time of transition. Legal operations professionals can assist with this feat by implementing optimal policies, training, and oversight. This ensures people understand why new processes and tools are necessary while also confirming compliance. For example, privacy laws that influence several functions are popping up around the globe. Automating document retention and contract review can be two ways that legal can work with other departments to help remain compliant with new regulations while also improving outdated processes. Change management can be an uphill battle, but having strong internal talent and leveraging external partnerships makes it easier to implement, explain, and sustain changing processes.

2. Creating roadmaps for new initiatives: When setting goals for the year, legal should determine what is valuable to the C-suite to create roadmaps for necessary tech adoption and process changes. These roadmaps should be customized for every organization, and can change depending on successes or failures. Make sure to designate individuals that employees can turn to for training and questions.

   Also determine what KPIs to set and metrics to track, and include these in the roadmap. Examples include how many deals legal helped sales close or any reduced litigation exposure from removing ineffective contract clauses. Things like this illustrate success along with cost-savings metrics. Simply put, knowing how the organization measures value increases the legal department's visibility which results in improved data optimization and tech scaling capabilities. This is another area where it may make sense to bring in an external provider that offers solutions with customizable dashboards, data libraries to benchmark against, and ongoing support for analyzing and presenting data.

3. Having the right people fosters successful automation: Whether having talent in-house or turning to external consultancies, organizations need the right legal operations experts who know how to implement their

tools effectively. Automation is key and allows the legal team to focus more on high-level tasks such as strategy and risk management. Without the right people in place, there is a greater chance that people will use new tools incorrectly. Many sessions explored the need for integration capabilities that help retrieve insights from even the hardest places (such as unstructured data sources), so that will be a desired commodity in the coming years.

4. Telling a story with data to demonstrate the legal department's value: Data is a source of truth as to how an organization is performing, and legal operations is the gatekeeper to this knowledge. In order to effectively tell a story with your data, the right processes and tools must be in place. Evaluate whether the organization has the capabilities and expertise in-house or if collaborating with a legal operations consultant would reach the end result faster with less internal lift.

   Talk to leadership to identify what information they want from the data. Prioritizing such initiatives will likely result in better buy-in for future projects and tech investments, allowing legal to continually innovate. Identifying where actionable data resides is the first step. Speakers noted that three major hubs are eBilling, eDiscovery, and contract management tools. Next, discover ways to repurpose data to inform other initiatives. For example, legal billing invoices can offers insights to help better understand spend allocation, forecast budgeting, track diversity efforts, or rewrite outside counsel guidelines.

   This is also where utilizing CLM software can be extremely valuable, as many struggle with managing or analyzing contracts effectively. Going through your contracts is important not only to implement better classification habits – but also to pinpoint inefficient or litigious clauses, draft better templates, determine if obligations can be prepaid at lower rates, reduce storage needs, remain compliant under new regulations, and quantify risk.

5. Legal operations professionals are a new breed that will transform the industry. One speaker noted that 78 percent of legal ops professionals are viewed as being cross-functional within their organizations. Because this is such a new area, many are creating their own roles and adjusting responsibilities as they go along. The focus should be on where legal operations teams can fill gaps and what creative solutions will help promote buy-in, effectuate meaningful transformation, and develop the necessary change management skills to get the best ROI and lessen operational pain points.

   Many legal operations professionals have strong eDiscovery backgrounds and are exploring how these skills can translate into other areas of the business – a notable one being contract management. Just like managing a large eDiscovery matter, it takes solid project management skills, the ability to create repeatable processes, and an understanding of how different technologies can be leveraged. While some have a legal background, others do not. This is why CLOC is key to fostering collaboration between innovative minds and molding the industry further. Members had an opportunity to hear stories about legal operations successes and failures, ask questions, and connect with individuals in this space to tap into collective innovation.

Conclusion

This is an exciting time in the history of the legal industry as the operations community grows. At CLOC, this enthusiasm was present in every session. With the role of legal operations expanding, people can work more efficiently and are fulfilled in their roles, cost savings emerge, and legal can finally be viewed as a strategic business partner crucial to an organization's transformation.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Data Intelligence and Analysis – The Importance of Upfront Analysis to Identify Key Information – The Role of the Lawyer/ Technologist

Taking extra time at the front end of a new matter will undoubtedly save time and money, but perhaps more importantly, can inform legal strategy moving forward throughout discovery and litigation.

Analyzing a data set during early case assessment (ECA) can unveil pitfalls that may not become evident until much further down the road, which can be devastating with large-scale matters that have a tight production timeline. Understanding the data characteristics of a given population ensures adequate time to remediate any data issues prior to production. It also affords an opportunity to assess the potential risk with regard to pending legal issues, as well as unknown and potentially damaging issues. In many instances, a thorough investigation will reveal key documents that afford the legal team an opportunity to perform tactical fact development and build their case before, or in tandem with, document review. Finally, this early analysis can identify challenges that may slow or impede a review, such as a high volume of privileged content, documents needing redactions and privacy concerns.

When consulting with clients, there is common concern about what should be the focus during early case assessment. This is a fundamentally sound question but probably one of the most difficult questions to answer in the abstract. This is because there is not a simple formula or universal blueprint that can be easily replicated. Each data set and the corresponding substantive case introduces unique elements that need to be examined in light of the specific end goal.

The first step, in almost every matter, is to examine the data through the lens of a machine. In most large matters, the data is going to be ingested into a review platform as well as an analytics tool. There are data deficiencies that pose problems with both, and any concerns should be addressed as early as possible. This step also means that practitioners should examine and assess the quality of the text. Although poor text can pose problems with simple searching, quality text is critical to any project that will leverage analytics. A more detailed analysis will consider the make-up of the data set from a file

type perspective, with consideration as to what documents will be supported by the review platform and analytics tools.

Understanding data from a technical perspective is key, but not the sole consideration. In an environment where litigation is increasing but pressure is mounting to keep costs low and maximize efficiency, it is imperative to perform a preliminary factual analysis to some extent, before executing a document review. Understanding the anticipated responsiveness level within your set, as well as the prevalent issues and potentially damaging documents should be a priority. Additionally, early insight regarding the estimated effort for a privilege review and log can set the stage for an informed strategy and a successful, well-managed document review.

The analysis should be performed by someone who is highly competent. In many cases, this is someone with a legal background, with subject matter expertise in the matter, who can issue spot and quickly identify the most interesting or inflammatory content. Ideally this individual will be proficient in legal technology as well as an expert in data interrogation and able to perform the requisite analysis. Enter the lawyer/ legal technologist. We have seen an increase in these types of roles at law firms and corporations and they are becoming essential to modern day eDiscovery. For those that do not have

a lawyer with these qualifications on staff, it becomes more important to partner with a trusted service provider that can provide guidance through the process or to execute on their behalf.

This blog post is an excerpt from the Chapter titled "Outsourced Document Review: Data Intelligence, Technologist Lawyers, Advocacy Support" by Edward Burke and Allison Dunham, which appears in the Thomson Reuters treatise eDiscovery for Corporate Counsel (2022). Reprinted with permission, © 2022, Thomson Reuters. Ed and Allison are eDiscovery experts at Epiq.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

How to Position Technology Assisted Review (TAR) With Government Regulators in Antitrust Matters

Regulators in the U.S. and abroad have been quick to recognize the value of technology-assisted review (TAR) workflows as important tools that can prevent massive data dumps and allow them to focus their analysis on critical and relevant data. A significant aspect of our experience producing data to government agencies has developed in antitrust matters relating to mergers and acquisitions. When the Government issues a request for additional information (referred to in the U.S. as a Second Request), parties have a limited time frame in which to collect, process, analyze/review, and produce a potentially large set of data, collected from an ever-expanding number of sources. In these circumstances, it would be challenging (if not impossible) to reach a point of substantial compliance without the use of tools that can quickly and defensibly identify potentially responsive data. Although some counsel may still favor the use of search terms to identify responsive content, the clear trend for complying with Second Requests in the U.S. is to deploy a TAR workflow.

The Antitrust Division of the Department of Justice (DOJ) requires counsel to provide information at the inception of the project regarding whether the party intends to utilize TAR as part of the analysis process. Counsel must provide such information as:

i. the identity of the eDiscovery provider,

ii. a description of the TAR process (including the TAR software deployed),

iii. the lawyers who will be training the algorithm,

iv. targeted metrics for recall and margin of error, and

v. the type of data that will be run through the TAR engine and identification of data that will not be included in the TAR process.

Given the need to quickly assess responsive content and to get it analyzed/reviewed in an expeditious matter, Standard Active Learning protocols (TAR 1.0) have become the accepted norm. Once the DOJ has signed off on the TAR Protocol, it then typically expects to receive and review several randomized sample sets of documents that fall below the TAR cut off score in order to validate the results of the TAR process. One significant benefit of the DOJ's approach is that the parties have a clear understanding, before they begin, about the details of the TAR process and how the results will be evaluated. Historically, the Federal Trade Commission ("FTC") has not required the same level of up-front negotiation and scrutiny into a party's proposed TAR methodology/process. However, in a recent blog post, the FTC indicated that it is moving to an approach that is more in line with the DOJ, and has begun to ask for a TAR Protocol at the inception of the matter. *Making the Second Request Process Both More Streamlined and More Rigorous During this Unprecedented Merger Wave*, https://www.ftc.gov/news-events/blogs/competition-matters/2021/09/making-second-request-process-both-more-streamlined?utm_source=govdelivery (Sept. 28, 2021).

Although these approaches are not necessarily indicative of how other government regulators will respond to the use of TAR when receiving data and what they will require, there are certain general points to bear in mind when producing to a government regulator or legislative body:

- Be sure to review and understand any operative ESI Protocol that the relevant agency or legislative body may have promulgated. Apart from the use of TAR, it is vitally important that legal counsel understands how to produce data to that agency. Any government requirements may also have an impact on how the document review process will take shape.
    - As an example, if an agency prohibits any "downgrades" of documents from responsive to non-responsive after the completion of the TAR process and the identification of a potentially responsive set, the best approach may be only to review the documents flagged as potentially privileged and those that were not run through the TAR engine.
    - This workflow has also become common for U.S. Second Requests. In that case, to better understand what is in the produced data, the responding party can perform analysis of the data set to be produced (after the TAR 1.0 process has been completed) using a Continuous Active Learning (TAR 2.0) workflow.
- Determine whether the agency requesting the production of data has requirements around the use of TAR. Even if not specifically required or set out in a policy document, it is always best to engage in these discussions with the government attorney who is assigned to your matter early in the process so that he or she has a clear understanding of how you wish to proceed. If the legal team is not fully familiar with the details and nuances around the use of TAR for productions to the government, they should feel comfortable including the outsourced eDiscovery provider on these calls or, at a minimum, having it provide guidance to counsel beforehand.
- The legal team should work closely with their eDiscovery provider to oversee the TAR process. The results of using TAR are always enhanced when there is a close working relationship between counsel and the eDiscovery provider.
- Be sure to follow any reporting requirements that the agency may require.

This blog post is an excerpt from the Chapter titled "Outsourced Document Review: Data Intelligence, Technologist Lawyers, Advocacy Support" by Edward Burke and Allison Dunham, which appears in the Thomson Reuters treatise eDiscovery for Corporate Counsel (2022). Reprinted with permission, © 2022, Thomson Reuters. Brett Beeman also contributed to this blog.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

U.S. Data Privacy Updates: Spring 2022

The time has come for another review of U.S. data privacy updates, as this landscape is growing and dynamic. Keeping informed ensures organizations know what is on the horizon and how new or amended legislation may affect business operations and compliance obligations. The absence of federal legislation elevates this task, as many organizations conduct business in several states with differing directives.

Back in January when the Epiq Angle last issued an update, the three states with enacted data privacy laws were California, Virginia, and Colorado. Other states had pending bills or were regulating via less comprehensive laws, such as Nevada's law pertaining to data broker sales. Below is a recap of what has happened in 2022 thus far and what may follow.

Utah Consumer Privacy Act

This March, Utah became the fourth state to pass comprehensive data privacy legislation. The Utah Consumer Privacy Act (UCPA) will become effective on Dec. 31, 2023. The law categorizes both personal and sensitive data. Following suit with the other three laws, the UCPA can apply across state borders and grants similar rights to consumers regarding personal data such as the right to access, delete, and opt-out of sales. It also places controls on organizations' processing activities such as notice and security obligations.

No private right of action exists, leaving California as the only state currently extending that right. Instead, the Division of Consumer Protection has investigatory powers, and the Attorney General (AG) has enforcement powers. Allotted penalties are $7,500 or the measure of actual damages. The UCPA provides a 30-day right to cure period before enforcement. Any enforcement-related funds go into an account the AG can use for enforcement and consumer education. The AG does not have rulemaking powers.

The UCPA overall has a more relaxed and business-friendly feel. Organizations falling under the law's reach should take note of provisions that make it less restrictive:

- Consumers do not have the right to correct erroneous personal information, which the Virginia and Colorado laws allow. The broader California Privacy Rights Act (CPRA) that will expand current protections also allows correction starting Jan. 1, 2023.
- Organizations are not required to perform data protection assessments, cyber audits, or risk assessments before engaging in riskier processing activities.
- The scope of when organizations can issue fees upon responding to consumer requests is broader.
- There is no requirement for organizations to establish a way for consumers to appeal decisions.
- Organizations must provide opt-out notices to consumers regarding sensitive data collection. Conversely, in Virginia and Colorado, this type of information cannot be processed unless a consumer opts in for collection.

This list is not by any means exhaustive, so as always, affected organizations should thoroughly review the law to inform proper compliance strategies. It will be interesting to see if other states follow Utah's approach and if the inclusion of fewer restrictions will lead to quicker legislation passage.

Pending State Bills

The majority of states continue to introduce data privacy legislation in each new session. As of May 23, there were 12 active privacy bills. Earlier in the year, almost 20 other states had proposed bills that did not pass. Some even have multiple on the table, such as Pennsylvania where three competing bills offer different restrictions. Some differences between the Pennsylvania bills include penalty allowances, limitations on consumer rights, definition for personal information, and authorizing a private right of action.

Connecticut is the state to watch right now, as the state's bill passed in both the Senate and House in late April. The governor recently signed the bill on May 10. Key features include no private right of action, sunset date on the right to cure, unique definition of biometric data, and broad consumer opt-out allowances. Watch out for any amendments or guidance before the law becomes enforceable.

The Virginia law was amended this April, even though it does not become effective until next year. The changes create a new exemption pertaining to a consumer's right to delete; replace the fund for penalties, expenses, and fees; and change the definition of "nonprofit" to include political organizations and any tax-exempt organization.

While not relating to comprehensive privacy protections, an emerging trend is the introduction of bills similar to the Illinois Biometric Privacy Act, which regulates how organizations collect, use, safeguard, handle, store, retain, and destroy biometric data. Some have already failed, but the California biometric bill is looking like the most promising one still pending to pass in the near future. Delaware and Massachusetts also introduced bills to specifically regulate data brokers, which is another specialized area gaining momentum.

Uniform Personal Data Protection Act

Last July, the final text of the Uniform Personal Data Protection Act (UPDPA) was approved. This is a flexible model law that states can adopt privacy legislation after. The UPDPA's approach is based on tort instead of looking at data as consumer property. The UPDPA views the consumer-business relationship as an exchange that benefits both parties. The goal is to still address consumer privacy concerns while significantly reducing burdens placed on organizations, which encompasses both costs and the ability to remain operational while still complying with the law. Major differences include the absence of consumer deletion and portability rights; varying privacy levels and consent requirements dependent on data compatibility categorization framework; and substituted compliance allowing implemented controls relating to another state's law to satisfy compliance in a state following UPDPA rules.

Nebraska, Oklahoma, and Washington D.C. legislatures have introduced UPDPA-modeled bills, but none have passed. Additionally, many states have incorporated provisions from the Washington state bill that did not pass. Virginia has a lot of the Washington bill's features that make compliance easier by taking a less onerous and mandated approach. It is crucial to watch whether more states propose and/or adopt legislation pursuant to the UPDPA framework or the Washington-Virginia model, and whether either option helps lessen the load of compliance or even spark creation of a federal standard.

Final Thoughts

Next year will absolutely be a major year for compliance program updates – especially considering the fact that other pending bills could advance and swing late 2023 effective dates. The Virginia law and CRPA both become effective in January 2023. The Colorado and Utah laws are not far behind with effective dates in July and December 2023, respectively. The Connecticut law is also slated to be effective next July. The patchwork approach to data privacy regulation in the U.S. renders it challenging to meet competing obligations when organizations operate in multiple jurisdictions, but it is necessary to avoid fines and reputational harm. Being proactive and implementing changes now better positions organizations to avoid violations and operational interruptions. Be sure to prioritize legislative monitoring in compliance initiatives, as things are evolving quickly and bills that appear promising today could prove invalid tomorrow.

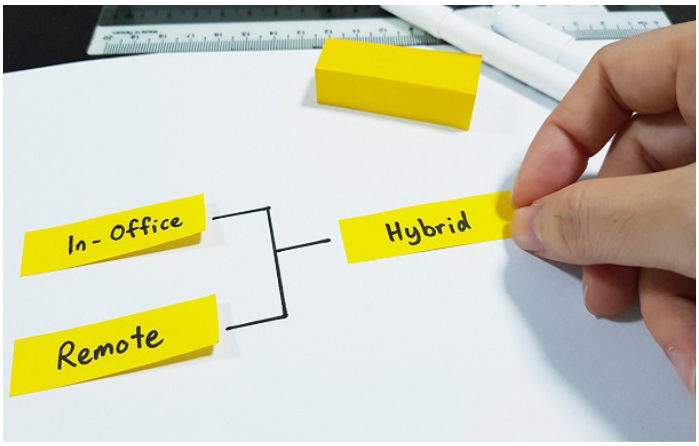
Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Five Critical Considerations in a Hybrid Work Environment: Information Governance

Information governance (IG) has never been needed more than in today's workplace. It is clear that remote and hybrid workforce models are here to stay, and emerging technologies to support this way of working are creating endless data sources for organizations to consider in their IG program.

For example, the adoption of collaboration tools skyrocketed over the past two years and will continue to remain an integral part of business operations for many organizations. With new technologies and information sources, organizations must strategize on ways to modernize vital records and data management practices to reduce risk and maximize value.



Considerations looking forward

While often viewed solely as a back-office function, a comprehensive approach to your records and information management strategy is now critical in the face of data expansion and mass digitization. Policy creation should be more strategic and flow through all departments, as everyone is responsible for maintaining proper information governance hygiene. Below are five things to account for when transforming information governance programs during these digitally-fueled times.

1. Accelerated digitization: It is well-established that the pandemic propelled many digital trends that were already materializing, such as moving away from paper documentation and increased remote work allowances. With many organizations across industries planning to continue operating off hybrid models, there are vital information management principles to revisit. Besides accounting for new data types and information repositories, there are other challenges teams may not have considered – one being how downsizing real estate affects retention policies. Less physical office space means less room to store hard copy documents. This provides an opportunity to dive deeper into retention policies and deploy innovative solutions such as automating document classification, updating digitization workflow and paper initiatives, and security storage enhancement. A strong program rests on a combination of technology deployment and policy development accounting for evolving workflows or digital habits.
2. Physical security challenges: While remote working offers compelling benefits, it also inherently increases risk. Bringing home corporate devices and records, using personal devices, and operating off home networks are a few components of this working model to address. Actions to consider that limit risk include VPNs, shared drives, automatic cloud backups, minimum internet requirements, policies regarding locking devices when left unattended, limited printing capabilities, digital mailrooms, and designated collaborations platforms for internal or external communications. Contemplate current and future business needs to determine which information policies make the most sense and reduce the security challenges associated with hybrid working.
3. Flexibility: While a certain rule may govern information habits, there is generally room for taking flexible approaches that vary between organizations, or even teams within a single organization. Factors to evaluate include globality, types of data collected and stored, risk appetite, and departmental priorities. This will help guide policy and procedure creation regarding information management and security. To maintain defensibility, ensure applicable rules and regulations are followed – such as adding extra security measures over certain document repositories where high-risk data is stored while implementing different processes for data requiring less oversight.

4. Compliance: Data security and privacy are two major compliance drivers that are transforming information governance initiatives. The rise in cyber threats and increasing ransomware costs coupled with emerging privacy regulations render it crucial to build out cyber and information management policies together. Method of reducing risk include creating internal compliance roles, consulting with experts in these areas, outsourcing compliance functions such as consumer responses to information requests, implementing new security standards for remote workers, and tapping into automated technologies.

Planning: The foundation of a successful program is assessment and planning. Now is a perfect time to reflect on how certain remote processes have been working and what information management challenges exist to better prepare for the future. Some things to consider are areas that would benefit from automation or outsourcing, internal role creation, which data can also provide insights to inform strategic moves, applicable regulations, and storage capabilities. A transformed approach to information management improves the ability to serve clients while also reducing associated costs and mitigating risk associated with data loss or exposure. Training and auditing are also key for role recognition, especially when introducing modern technology and balancing remote capabilities. Equally as important, ensuring you are educating stakeholders on compliance best practices is necessary. Finally, consider document management system health checks to audit the current state of governance and storage operations and how hybrid work factors into these processes. This illuminates improvement areas to address in future information governance initiative planning.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Rising Interest Rates and Restructuring Predictions

In an effort to combat inflation, the Federal Reserve (Fed) is raising interest rates. Inflation is a decrease in the purchasing power of our money which causes prices to increase in goods and services over time. The pandemic has presented added challenges such as labor shortages, the onset of COVID variants, and changed consumer habits adding pressure to deliver goods and services in high demand. As predicted, the Fed recently hiked interest rates by a quarter point percentage in March and again by a half percentage point in May. Rates are expected to climb as high as three percent by the end of 2023. This is the biggest hike in over 20 years.

The logic behind this move by the central bank is that higher interest rates will decrease demand thus allowing prices for goods and services to stabilize and drop back down. Many economists argue that the recent action by the Fed to curb inflation may be too late and the increase in interest rates for corporate borrowing may cause a recession while others believe that our economy is strong enough to curb inflation without crumbling. Regardless of direction, raising rates will likely cause an increase in restructuring agreements.

The State of the Capital Markets and Labor Market

Over the past two years, the amount of funds available to businesses facing challenges has been unprecedented. The federal stimulus relief funds coupled with lenient lending policies have allowed businesses to survive and sometimes thrive during the pandemic. As we recover from the challenges of Covid, longer lasting ramifications of our "easy-money" environment may be upon us. We could be heading into a more turbulent economic period which could ultimately resemble an economic recession. Some companies may need to restructure their balance sheet or operations or both. To better understand why some companies may be forced to considered restructuring options, let's look at some key dynamics: the current position of capital markets, supply chain issues, and the status of our labor force. Below is a brief analysis of how the U.S. is faring in these areas just over two years into the pandemic:

- **Capital Markets:** The economy refers to the wealth and resources of a particular area in terms of production and consumption of goods. Distinguishable from this, capital markets absorb thousands of external data points in real time. Then, these financial markets react accordingly by setting a value to an organization's equity price. With anticipation of the Fed rising interest rates, stock prices and cryptocurrencies have already dropped. It is safe to say that these markets will experience volatility for a while. Since risk is always factored into the stock market, most analysts expect a quick recovery when inflation gets under control – especially if the economy remains strong.

- **Labor Markets:** The labor market may appear to be bouncing back, but it is still weakened and in flux. While unemployment numbers have steadily decreased and many organizations are recovering, this is not indictive of the market's overall strength. Other variables factor in that contribute to slower recovery such as the onset of Covid variants, unknown future spikes, and labor shortages. To retain talent and remain competitive, many organizations are increasing wages which can also add to inflation issues.

- **Supply Chain:** The pandemic has disrupted every aspect of our global supply chain for raw materials to finished consumer products. We are now very aware of our supply risks and vulnerabilities as Covid has highlighted these past two years. Companies are looking to build resilience and new sourcing, but some will not be well suited to

change models to meet demand. Forecasts indicate that these challenges will continue through 2022 and possibly beyond.

Corporate Restructuring Predictions

Even if capital markets bounce back and the labor force completely rebounds, restructuring will be necessary for some organizations to survive. Interest rate increases, continued inflation, supply chain issues, and the unstable labor market all will likely contribute to more restructuring activity in general. Trends that are likely to emerge during the second half of 2022 and 2023:

Many distressed organizations have successfully fended off bankruptcy filings by borrowing funds at attractive interest rates over the past few years. Some also received federal stimulus relief. As interest rates increase, access to the capital markets will tighten making future borrowing or debt amendment difficult. Both the interest rate on loans and fees associated with obtaining loans could be an insurmountable challenge. To remain viable, organizations in this position that have not returned to pre-pandemic operations may need to restructure assets out of court or seek bankruptcy protection.

Lenders will work with corporate borrowers to find reasonable solutions, but many will look to exercise their contractual rights which include foreclosures and asset seizures. Overall, lenders will be more aggressive than they have been over the past two years. Undoubtedly, work out groups at banks and non-traditional lenders will become more active in assessing the value of businesses in the post pandemic environment. Any inability to repay secured obligations would likely result in companies seeking an out of court restructuring or a formal chapter 11 proceeding.

While many organizations will remain stable during this time, others will fall into the categories listed above. For those that experienced recent financial headwinds, it is crucial to evaluate financial positions to determine the best path to take in order to thrive.

If you enjoyed this article, consider reading Where to Next? Travel and Bankruptcy Predictions Remain Foggy

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Five Qualities to Look for in a Third-Party Administrator

Financial institutions can face investigations from a number of regulatory bodies such as the Federal Reserve, U.S. Department of Justice, U.S. Securities and Exchange Commission, and Federal Trade Commission. Common topics of inquiry include discrimination during the mortgage process, compliance with applicable federal and state laws, and much more. There has been increased scrutiny during the pandemic to ensure consumers are not being taken advantage of by a financial organization. Oftentimes, investigations from these regulatory bodies can lead to a voluntary remediation, Matter Requiring Attention (MRA), or public consent order.

When a settlement is needed, reaching an agreement on terms is just the beginning of effectuating proper compliance. Organizations often encounter tight deadlines and requirements to quickly implement a customer remediation program. When this is the case, selecting and retaining an experienced third-party administrator (TPA) is beneficial. While this can be handled internally, that route diverts valuable resources, may require additional staff, and lacks the expertise a seasoned TPA can offer.

When selecting a TPA to partner with for regulatory settlement administrations and voluntary remediation programs, evaluate the following qualities:

- **Regulator familiarity:** Each regulator will vary with what they require in terms of deadlines and supervision. Established administrators have developed an understanding of regulatory rhythms based on prior matters. Look for an administrator that has the experience to assess how a regulator may respond to various remediation approaches and can assist in presenting a persuasive case. This can save a financial institution both time and money by understanding and meeting the needs of the regulator from the onset versus figuring it out along the way.
- **Proven experience:** In addition to regulatory familiarity, a TPA's record of achievements speaks volumes. It not only shows they can get the job done well, but that they have the capacity to repeat outcomes, respond quickly to requests, adjust to changes, and efficiently handle late-breaking requirements. This can include handling more complex or bespoke requests from financial institutions or regulators as they arise. Oftentimes, an investigation will require an array of subject matter knowledge so being proficient in several areas is compelling.

- **Ability to maximize consumer participation:** Many regulators aim to provide redress to as many consumers as possible, oftentimes looking for a participation rate in the 70 to 90 percent range. This can be a high bar without the proper teams and processes in place especially when a substantial number of affected accounts have been closed for several years or there are other communication obstacles. Look for a TPA that can help meet this goal as part of the remediation program by offering flexible communication capabilities, ADA compliance, multi-language support, and documented complaint handling procedures.
- **Appropriate payment tools:** Working with a TPA that leverages innovative tools is key to accurately issuing payments in a streamlined manner. Technology can play a key role in driving high participation rates, making payments quickly and securely, and providing insights into valuable metrics. Enticing offerings include electronic noticing and payment reminders, nimble and flexible call center technology, electronic claims adjudication, and digital payment solutions.

- **Security capabilities:** Safeguarding consumer information is more important than ever before with all the risks present in the digital world and emerging privacy regulations. Look for a TPA that places security as a top priority and utilizes the right tools to support this goal. Best practices include offering secure disbursement software, fast and secure digital payment solutions, trusted security personnel with industry certifications, multi-layered physical access security, security monitoring, and other data protection tools.

Remember that a TPA can help financial institutions achieve remediation goals, satisfy the terms of an agreement, save costs, and end the heightened scrutiny an MRA or consent order entails. Leveraging their expertise can also inform future decisions to limit the risk of subsequent investigations. Consider utilizing this partnership not only for investigatory support, but also to update compliance and risk management efforts.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Counsel and the Breach Response Lifecycle: Best Practices at Every Stage

The shift to automated business processes and digital data management has definitely been a key enabler for organizations across industries. This fosters more efficient transactions, saves on costs, reduces time spent on projects, and helps organizations maintain competitive. With digitization also come increased cybersecurity risks. Data becomes more vulnerable to interception, potentially leading to legal, regulatory, or other compliance violations. It is important for organizations to have a dedicated incident response team that can detect breaches earlier and quickly jump into action if one materializes. A breach creates a chaotic time for any organization, so having a tested plan that delineates key actors can help limit the fallout and streamline remediation.

Involving counsel during strategy talks and tabletop exercises will limit risk by considering important legal implications from a breach in advance. Collaboration between legal and cybersecurity teams prior to a breach has been lacking historically. Some areas counsel can weigh in on include what data will be more vulnerable or targeted, breach notification obligations, regulatory and legal compliance, anticipated deadlines, communication phrasing, reporting, privacy considerations, and applicable contract clauses. Best practice is to proactively outline counsel's role at each stage in a breach response plan.

Taking a closer look, here are some ways to do so:

- Identification: After detecting a breach comes the investigatory phase where the response team needs to identify and analyze scope, attack location, threat actor information, type of data that was stolen or compromised, affected operations, and any other crucial information. At this point, the team should already know who to notify from legal and have relevant contact information. Make those calls immediately so counsel can advise on applicable laws, regulations, and contractual obligations. This will dictate what needs to be preserved, where legal holds apply, reporting requirements, and who to notify. This also supplies protection from spoliation claims in the event of future litigation stemming from the breach and a realistic timeline for the team to follow. The team can then work with a partner using trusted technology to cull the data set down to include only what is needed for notification and remediation purposes.
- Containment and Eradication: Next, the response team must act quickly to contain the breach in order to limit exposure. This includes technical measures such as isolating servers and changing passwords. Shortened containment cycles will significantly reduce overall breach response expenses, so tools that streamline this process add significant value. Eradication is necessary before restoring affected operations. Hardening security, removing any artifacts associated with the breach, and making necessary updates is what occurs during the technical side of the eradication stage.

  While it may be difficult to envision counsel's role during this highly technical stage of breach response, this cannot be discounted. During containment and eradication, more information will likely come to light regarding compromised data that contains sensitive information. This, along with the already culled data set, should be sent to legal and escalated to the review team. It is crucial for counsel to collaborate with the review team on which information to extract and any relevant deadlines.

- Notification and Reporting: After creating a final notification list, time is of the essence. Reaching those affected by the breach needs to be done quickly, thoroughly, precisely, and reliably. The internal team or outside provider will perform final contact verification, send out appropriate notices, set up a call center, and establish credit-monitoring services if needed. Collaboration between counsel and any provider assisting with remediation is necessary to align notification with compliance obligations.

  Incident response teams need to consult with legal regarding any unique notification or reporting requirements. This can require action earlier in the process than when consumer notification occurs. For example, the GDPR requires an organization to notify the appropriate supervisory authority without undue delay and within 72 hours after discovery, when feasible. Counsel should help facilitate this process to reach appropriate regulators and meet any additional content requisites. Legal can also help with cyber insurance reporting obligations, which will come into play throughout the entire breach response lifecycle. Lastly, counsel can opine on whether press releases or image rebrand are necessary, and what that should entail.

Factoring the above into breach response strategy will help anticipate response needs and workflows, allowing teams to create or alter plans so they are thorough and legally defensible. After an incident occurs, the aftermath can be a long process. Having an established plan, involving counsel at every stage, and collaborating with vetted provider partners all helps streamline the process. Remember to document efforts and legal advice to maintain compliance and defensibility. In the event future litigation ensues stemming from the breach, there will already be attorney-client privilege established regarding breach response efforts and greater defensibility on process.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

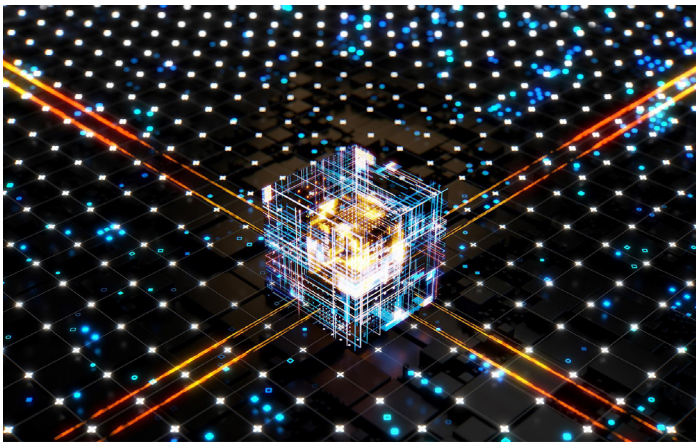
The Importance of Using AI Effectively and Transparently

Artificial intelligence (AI) is everywhere, and most people use it on the daily. From facial recognition software allowing access to mobile devices to recruitment technology that helps human resources departments vet candidates, this technology is versatile and complex. In the legal space, AI has emerged most frequently in litigation and regulatory contexts. Examples include solutions that streamline and improve efficiency with document review during investigations or discovery and litigation analytics to inform decisions such as the probability that a motion will be successful before a specific judge. In all these scenarios organizations and their legal counsel have important responsibilities to use AI effectively while remaining ethical, especially when dealing with challenges to any data judgement calls. Being transparent about the tech selection process, manual oversight, and technical aspect of the AI solution used can help organizations maintain compliance.

AI from a Business Perspective

Integrating AI usage as standard practice can raise efficiency for many processes. For example, being able to use predictive technology to find suitable candidates for hiring vacancies can significantly cut down on time and fill spots quickly. Organizations with high volumes of contracts can also realize time and cost-saving benefits when using AI software to not only manage their contracts but also take a deep dive into key issues affecting negotiations or compliance – such as effects of a new regulation or force majeure applicability. For litigators, using AI for early case assessment can inform strategy and guide key decisions including when to settle or which documents to preserve to avoid future spoliation claims. These are just a few illustrations affirming that AI can be very useful across every industry. The question then becomes: when is it worth it to invest in AI from a business standpoint?

To answer this question, organizations need to ponder when AI will be most effective. Beneficial features to look for when investing in new technology are whether it will add business value, increase efficiency, enhance current processes, reduce costs, and manage risk. Some ways to gauge this are through solution comparison, benchmarking, tracking performance



metrics after deployment, or business transformation consulting. Remember that it may take some trial and error to find what combination of people, process, and technology is optimal.

Even when organizations feel AI investments are economical and effective, ensuring practices remain ethical and meet all legal obligations is crucial. This means at minimum having a basic understanding of how technology operates to explain decisions. While a challenging feat since AI is so complex, failure to consider technical aspects before and after investing will be problematic because there is a trend of explainable and transparent AI emerging in regulatory matters which will likely expand.

Transparency Obligations

AI is great for automating processes, tapping into business intelligence, and managing costs. However, this type of technology is not intuitive by design which makes it difficult to explain. Take the example of AI recruitment software. If an organization is faced with a claim rooted in discrimination, it will need to be able to explain the technology behind the decision as part of their defense. While the manual training component helps, ambiguity exists around how the software processes this data and makes judgements to support the

results. This is where the ethical quandary comes into play – as clients, consumers, regulators, or the courts may want access to the data and processes backing decisions. Additionally, the General Data Protection Regulation (GDPR) grants a legal right for consumers to have AI explanation when an automated decision significantly affects them like with the hiring example noted above. Similar and stricter obligations are also materializing, such as China and the EU's proposed algorithmic regulations.

With these obligations trending globally before regulatory bodies and courts, it is critical to minimize risk by finding ways to make AI better explainable. While this will always be a very technical and often challenging battle, here are some best practices to consider:

- **Incorporate transparency into research:** When vetting an investment, see if there is any information available that indicates issues or improvements with a certain solution. Organizations should look at public studies or testing data, talk to colleagues, consult with industry experts, or meet with counsel before making an investment to ensure their preferred AI systems promote transparency.
- **Consult with counsel and provider partners:** It is crucial to factor ethical AI usage into information governance and risk management initiatives. Counsel and providers helping with data governance or business transformation are beneficial resources. They can consider applicable legal and regulatory obligations applying to AI automated decision making imposed by court decisions, the GDPR, other privacy laws, consumer finance regulations, and more. Additionally, they can consult on best practices or create standardized templates for documenting AI model creation and training.

Also consider creating an AI Explainability statement, the first of which emerged in 2021. The purpose of this statement is to increase and support transparency. It should include the reasons for using AI, how it functions, logic behind decision-making, training components, and system maintenance. An organization should update the statement when necessary and as more organizations publish them, best practices for what to include will evolve.

- **Monitor key AI updates:** Look out for whether more organizations publish AI Explainability statements and what they include. Also pay attention to any amendments or delays with the proposed algorithmic regulations discussed above, as this will be instructive for other countries wishing to regulate this technology. While there has not been a flood of data protection decisions regarding transparent AI, there have been a few [cases?] before GDPR enforcement agencies over the last two years. If an upward trend continues in this regard, more organizations will need to enhance AI transparency practices. Getting ahead of the curve will save this headache down the road and help ensure that operations relying upon automated technology remain ethical and defensible.

To learn more about how Epiq can help you use AI, click here.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

How will the Metaverse Influence Business and Legal Processes?

The metaverse is the latest hot topic when it comes to predictions for the next iteration of the Internet. Several big tech and gaming companies are investing in this space to build it up. It should be a best practice for organizations in every industry to monitor progress made in the coming months and years. So, what exactly is the metaverse? While still a working concept and not completely defined yet, the simplest description is an immersive, three-dimensional shared virtual space allowing users to interact with one another as if in person. But the metaverse is much more layered than this, and it will likely function as a standalone digital economy with open access for users to participate in the continuous evolution. Augmented reality, digital currencies, and other advanced technologies will fuel the metaverse.

Potential Business Applications, Challenges, and Risks

Some organizations have already started participating in the initial stages of the metaverse by opening banks, hosting virtual law firm offices, and creating retail strategies. There will be many opportunities in the future as this space evolves. Entering the metaverse will provide organizations much more than typical remote communication tools like video and text chat. Colleagues and clients can put on headsets and be taken directly into a virtual conference, meeting, or business transaction with individuals located across the globe. Interactions and visuals will be as if everyone involved was physically present via digital avatars.

While some will be hesitant to use the metaverse and adoption is difficult to predict, it is not going away and will undoubtedly affect internal processes, business dealings, case strategy, and more. Organizations should start thinking about the possibilities now to be better prepared for future challenges. Below are some predictions on how the metaverse will influence operations, strategy, and investments across different areas of the enterprise.

1. **Metaverse participants will need to revamp information governance programs.** Organizations participating in the metaverse or that have business dealings involving data from the metaverse will need to create new information governance initiatives. There will be massive amounts of data relating to a single transaction or interaction in the metaverse. Think about how much technology will be involved in a virtual office meeting to create rooms, avatars, and more. While these interactions may prove beneficial, risks will emerge in terms of managing data and keeping compliant with various legal, contractual, and business obligations. Organizations must account for this when strategizing about whether to invest in the metaverse, creating data retention policies, classifying data, using cloud storage, and setting data protection protocols. While organizations should already be considering these factors in their information governance initiatives, the amount and type of data involved in the metaverse will require reevaluation and present new challenges.

2. **The legal community will be faced with new eDiscovery challenges and ethical obligations.** Lawyers, legal service providers, and review teams should anticipate unique collection and review obstacles when data relevant to litigation or investigations resides in the metaverse. Challenges to prepare for include the need to use virtual reality (VR) headsets to view and analyze data, custodian identification, preservation mechanisms, and increased spoliation claims. Court decisions in this area will be instructive but it will be years before meaningful case law trends emerge.

For lawyers, ethics comes into play here as well as most states follow the American Bar Association's stance on competence – that requires lawyers to stay abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology. To avoid eDiscovery headaches in the future and remain ethical, best practices include metaverse and VR headset education and training, monitoring modern technologies used to power the metaverse, competitor analysis, and paying close attention to early case decisions.

3. **Cybersecurity risks will increase.** With so many moving parts and layered tech needed in the metaverse, cybersecurity is a top concern. Hackers will look for vulnerabilities as this space evolves and new attack methods may begin to trend. Organizations transacting in the metaverse must elevate cyber risk analysis and may need to implement stronger security controls to protect consumer data, trade secrets, and other sensitive information. While emerging technologies always invoke the need to evaluate cyber risk and identify potential gaps, the metaverse delves into unchartered territory. Consulting with cyber experts would be prudent to gain insights on the best way to keep data secure in the metaverse and limit breach potential.

4. **Application of privacy regulations will get tricky.** Comprehensive data privacy laws continue to pass around the globe. Data in the metaverse will invoke privacy concerns on a large scale as the tech used will collect biometric identifiers, health information, and other sensitive data. The amount of data organizations will be able to access will be greater than ever before. This can result in more targeted advertising, data sales, and storage needs.

How regulations will apply in the metaverse remains unclear. Which state or country's privacy law will apply if a transaction or interaction occurs solely in the metaverse and that is the only place data is stored? Will regulators need to amend laws to account for application in the metaverse? Will they need to create entirely new metaverse-focused privacy laws? How will interoperability affect application and designating controllers? Complex questions like this will continue to surface as the metaverse grows and adoption spreads.

Conclusion

As the metaverse evolves, organizations will gain more clarity about responsibilities and risks. It may take a while to get there, and adoption could be more prevalent in certain industries. However, over time most organizations will encounter the metaverse in some manner. Key areas to monitor include business uses, integration capabilities, interoperability, technology used to power the space, breach trends, and eDiscovery case law. It will be interesting to see how the metaverse takes shape, plays a role in business matters, transforms strategies, and fosters collaboration on a new scale. Keeping informed and prepared will help organizations make smart investment decisions, analyze risks, stay competitive, and procure optimal benefits.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Key Ethical Obligations in the Era of Modern Law

To achieve modernization, the legal industry is operating off a new mindset requiring focus on efficiency and innovation when making operational decisions. Legal departments, law firms, legal service providers, and other legal professionals are being more strategic with tech investments and partnerships. Many are revamping budgets, hiring or consulting with legal operations experts, refocusing goals, and determining ways to uncover data-backed insights. Throughout this transitional period, it is important not to forget the ethical obligations that lawyers owe their clients. These duties will influence tech investments and collaborative partnerships. While change is necessary and beneficial, it must be done carefully to avoid ethics violations that could provide reputational harm not only to the lawyer, but also the organization.

The American Bar Association (ABA) has model rules that most state bars follow closely.

Here are four key ethical obligations that should remain at the forefront of decisions when venturing into modern law and setting legal transformation goals:

1. **Competence:** ABA Model Rule 1.1 requiring competent representation recently expanded, clarifying that lawyers must keep abreast of changes in the law. This encompasses the benefits and risks associated with relevant technology. As the legal industry moves into modern law, these duties arguably require that lawyers at a minimum keep informed about innovative trending technologies and basic features to remain competent. Lawyers must diligently research new technology and/or the reputation of potential partner providers before investment. Failure to do so could result in an ethical violation if issues result after utilizing news tools for a case. Understanding benefits and risks also helps the legal team make educated decisions about where to allocate legal spend and confidently demonstrate these choices to leadership.

2. **Communication:** ABA Model Rule 1.4 requires transparent communication so clients can make informed decisions regarding representation. As legal teams decide to implement modern technologies or outsource case functions, clients must receive notice in the initial agreement and throughout the course of representation as needs evolve. Being transparent also demonstrates value to clients, fosters collaboration, and helps avoid major billing disputes.

3. **Confidentiality:** ABA Model Rule 1.6 mandates that client information be kept confidential. In accordance with this duty, the legal team must ensure that utilized tools are secure and will protect sensitive client data. This needs to be a top priority when vetting modern technologies and provider partnerships.

4. **Oversight:** Partnerships with alternative legal service providers (ALSPs) are trending in legal departments with the increased focus on operational efficiencies. Now law firms are starting to collaborate with provider experts for certain functions. The rise in collaborative business models coupled with ethical legal duties makes it crucial for lawyers to oversee work performed by any outside partners. Several ABA rules hold lawyers responsible for the work of their team. This extends to in-house support staff and external providers.

The ABA has formally authorized outsourcing legal and nonlegal support services when lawyers maintain competent representation, comply with duties related to supervision and assistance, notify clients, and receive informed consent from clients if the provider will be handling confidential data. However, there are specific state bar opinions on this subject that may vary.

One function many states have addressed is cloud computing, but with the uptick in ALSP usage there are endless possibilities. Predictions on future opinion topics include privacy considerations when outsourcing or the role of legal operations professionals. In the meantime, organizations should vet and audit their provider partners and technology to ensure everything is above board. This is an important step regardless to monitor success for meeting legal transformation goals and lessen the risk of ethical complaints from clients or delayed matters due to insufficient processes.

Given that that remaining ethical is the cornerstone of legal practice, as lawyers take oaths to act in accordance with the law and represent their client's best interests. In this dynamic space where modern technology continues to enter the market, ethical duties will keep evolving and new ones will emerge. Now more than ever, lawyers must keep on top of ethical obligations to avoid hurdles for organizations when investing in legal tech or changing processes. Monitoring relevant ABA and state court model rules, opinions, and court interpretations helps accomplish this feat.

If you enjoyed this blog consider reading ABA Issues Opinion - How To Respond to Data Breaches.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Best Practices for Positioning TAR in Antitrust Litigation Matters

In the early days of Technology Assisted Review (TAR), lawyers were sometimes hesitant about discussing TAR tools with opposing parties and the courts. Apart from a general concern about their ability to explain how the algorithms underlying predictive coding tools operated, litigators were unsure about what information to disclose and how to negotiate a "TAR Protocol" with opposing counsel. A number of courts quickly took the position that they would not micromanage the TAR process, but rather would encourage the parties to work together. The producing party generally determines the best way to produce documents and the receiving party can challenge this if it deems the production to be insufficient.

Key Case Law

Two decisions have proven to be instructive on this topic:

- *In the case Dynamo Holdings Ltd. Partnership v Commissioner of Internal Revenue* 143 T.C. 183 (U.S.T.C. Sept. 17, 2014), a Tax Court stated: "[T]he Court is not normally in the business of dictating to parties the process that they should use when responding to discovery. If our focus were on paper discovery, we would not (for example) be dictating to a party the manner in which it should review documents for responsiveness or privilege, such as whether that review should be done by a paralegal, a junior attorney, or a senior attorney." The Court went on to note that the respondent can always file another motion to compel if the production appears incomplete.

- *In Winfield v. City of New York, 2017 WL 5664852 (S.D.N.Y Nov. 27, 2017),* the Court directed the City to complete a linear review of the documents of certain custodians, and to also begin using TAR software "to hasten the identification, review, and production of documents responsive to Plaintiffs' document requests." The Plaintiffs objected to the City's continued use of its TAR approach and contended that the system was not properly trained because the City's human document reviewers over-designated documents as non-responsive during the linear review and TAR training stages. As a result, Plaintiffs asserted that the TAR software was unable to recognize and properly categorize responsive documents.

The judge disagreed, allowing the producing party to evaluate procedures, methodologies, and technologies for its own production as it was generally better equipped to make this decision. The Winfield court recognized that micromanaging internal review processes could reveal work product, litigation tactics, and trial strategy. Perfection was not required. The producing party just needed to advance reasonable and proportional production efforts.

Best Practices

The case law above has remained solid guidance over the years even with technology advancements. Here are four points to consider when deciding whether to deploy TAR and other types of analytics tools in litigated matters that can streamline the process of assessing and reviewing data during litigation:

1. At the inception of a new matter, work closely with your eDiscovery partner to discuss the facts of the case, type of matter, case themes, financial implications, and overall importance to the organization. These details are helpful for making recommendations about which analytics tools may be beneficial in litigating the case.

2. Discuss the types of data that may be involved in the matter. Certain types of data may not lend themselves naturally to the use of analytics tools, such as CAD drawings or financial spreadsheets. Newly emerging data types like Teams or Slack will likely have specific requirements around collection, as well as the processing, analysis and review. It is important to have a thorough understanding of the type and scope of data involved in the case before deciding how to proceed.

3. Be upfront with opposing counsel about the intention to use TAR solutions. Consider disclosing details about the TAR process without limiting the producing team's flexibility in deciding how to proceed. Common disclosures include the name of the analytics tool, the proposed workflow, and the types of metrics shared at production. It is uncommon for parties to agree to defined statistics, shared training, or specific training documents. The producing party generally does not need to share information considered work product or that would influence TAR training.

4. The focus has shifted from an upfront debate about the TAR protocols deployed to an analysis of the actual produced data. Although courts have not been willing to dictate how parties should proceed, they have been amenable to considering whether the production was complete if the production is challenged. Producing parties should be able to explain methodologies in the event of a challenge and receiving parties should understand that their right to challenge production is in no way affected by TAR usage.

Keeping informed of new case law and emerging technology trends will help counsel better position TAR effectively in litigation. Cooperation and transparency can help streamline matters and avoid the time and cost associated with extra motion practice.

This blog post is derived from the Chapter titled "Outsourced Document Review: Data Intelligence, Technologist Lawyers, Advocacy Support" by Ed Burke and Allison Dunham, which appears in the Thomson Reuters treatise eDiscovery for Corporate Counsel (2022). Reprinted with permission, © 2022, Thomson Reuters. Brett Beeman contributed to this blog.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Planning for a Remediation: Proactive Considerations for Financial Institutions

Financial institutions are more regularly dealing with voluntary remediations and public consent order activity due to heightened scrutiny by regulators and changing internal policies. These events can be complex and also time consuming when unprepared. In the age of efficiency, this is just another area to invest time creating flexible strategies. Being proactive positions financial institutions as better equipped for future remediation, restitution, and distribution needs.

Whether going off a consent order or implementing a voluntary remediation program, it is important to have workflows in place that drive quick and impactful resolutions. The goal is to get as many affected parties paid in the most efficient manner, so organizations do not waste valuable resources and their daily operations remain intact.

While process and compliance obligations will look different depending on the regulator and matter specifics, the following factors come up repeatedly in many remediations involving financial institutions:

1. **Digital Payments:** There is a trend towards digital payments as an alternative to paper checks. This is revolutionizing the payment process. Recipients have a streamlined choice on how to receive settlement payments – from direct deposit to digital gift cards. Remediation teams should be thinking through the value of partnering with a provider that can offer digital payments so that they can easily deploy the solution when restitution needs arise.

2. **Delivery:** Utilizing an automated solution with tracking for mailings expands capabilities and allows teams to handle higher volumes quickly and efficiently. Key benefits include scalability options, better notice, accelerated check cashing rate, cost-effectiveness, and reduction in post-distribution expenses. Having a partnership in place directly with the carrier or through a legal service provider makes delivery one less thing to worry about during the remediation process.

3. **Complaints:** It is beneficial to have pre-established game plans for situations involving supervisory inquiries, client complaints, lawsuit threats, or media coverage. Think through management strategies and which types of issues would invoke a complaint. Consider which complaints should be fast-tracked, require involvement with other departments, or necessitate a third-party partner for complaint management. This helps implement oversight practices, clearly delineate response roles, and create workflows that allow information to safely flow between each party.

4. **Tax Reporting:** Understanding the basics about when a payment will be considered income, withholding issues, and when to issue tax information returns can go a long way. Having internal counsel or an external partner in place to contact that can answer more complicated questions about tax treatment will also help eliminate delays during the remediation process.

5. **Bankruptcy:** This is another instance where it is beneficial having internal staff or external experts to offer advice, as bankruptcy accounts will require special treatment. Some things to proactively contemplate are how to treat different types of bankruptcies, administrative noticing and payment requirements, tax reporting, and ways to reduce risk related to double payment.

6. **Claims:** When consequential harm occurs, there may be claim-based remediation requiring additional non-monetary restitution such as credit monitoring or loan modification. This can be a complex and layered process. It is important to be aware of extra documentation requirements, legal hold applicability, appropriate release language, and how the appeals process functions. Align expectations with legal and outside partners before faced with a claim-based remediation to foster speedy resolutions if one arises.

Following the best practices outlined above for these six areas can greatly improve remediation efforts. Creating process and aligning expectations before an issue arises will streamline compliance efforts and ensure successful distribution to current and past clients.

For more in-depth information on this topic, consider downloading our latest whitepaper on this topic here.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Mandated Cyber and Privacy CLE for New York Attorneys – Will Other States Follow Suit?

The majority of U.S. states require attorneys with active law licenses to complete continuing legal education (CLE) credits. The number of hours, reporting deadlines, and topic requirements differ between jurisdictions. It is not only important for attorneys to remain educated on practice-specific updates, but also industry-wide legal trends and ethical obligations. Doing so helps ensure they have the tools and information available to provide superior client representation.

The Duty of Technology Competence

Since the American Bar Association updated their model rules to include technology competence a decade ago, three states have incorporated technology training mandates into their CLE requirements. While Florida and North Carolina allow a variety of topics to satisfy this training mandate, New York recently instituted more specific requirements applying to cybersecurity, privacy, and data protection.

Living in the digital age has placed cybersecurity concerns at the forefront of operations for organizations situated in nearly every industry. Going digital means that hackers can have easier access to data unless the processes and tools that safeguard this data are updated. While the move to automated business processes and digital data management has been a key enabler for businesses, it comes with increased cybersecurity risks. The common adage in cybersecurity is, "It's not if you will be breached, it's when.

The privacy landscape is also growing and dynamic as new jurisdictions continue to pass laws placing additional obligations on organizations that manage consumer data. Keeping informed is crucial to understanding how new or amended legislation may affect business operations and compliance obligations. With confidentiality being the cornerstone of legal practice, there is a heightened expectation that attorneys understand trending cyber and data privacy risks, as well as tools that mitigate exposure. This education is necessary to remain ethical and effectively protect client and other proprietary information.

New York Updates

This June, the New York Supreme Court adopted CLE requirements that the New York State Bar Association's Committee on Technology and the Legal Profession proposed. These changes account for the cyber and privacy concerns discussed above and will be effective on July 1, 2023. Attorneys must obtain one hour of CLE credit every two years on the ethical obligations, technology, or practice considerations relating to cybersecurity and privacy topics. This includes a focus on protecting client data and conversations, which is the foundation of attorney-client confidentiality.

The reasoning behind this update was to shift focus to pressing issues in the legal industry relating to data protection. Law firms and other legal organizations house a significant amount of proprietary client information including communications, case strategy, financial data, trade secrets, and more. If a hacker obtains access to a legal organization's systems or email accounts, the fallout can be monumental. Accounting for applicable data privacy laws adds an extra layer of compliance duties relating to this information. Incorporating education on these topics is meant to help attorneys understand not only their obligations, but also the proper safeguarding of sensitive data and incident response best practices.

Conclusion

With cyber and privacy concerns trending throughout the legal industry, it is likely other states will copy New York's CLE update. Keep tabs on Florida and North Carolina in the coming year, as they already have the generalized technology education requirement. It will also be interesting to see what the feedback is from New York attorneys after the initial reporting cycle that incorporates this update, and if that eventually leads to an increase in mandatory privacy or cybersecurity CLE hours. Even if other state bars are hesitant to mandate topics for education, there will definitely be an uptick in cyber and privacy CLE course offerings. At recent legal conferences, these topics have already begun to dominate sessions – and with good reason. All legal professionals need to understand trends in these areas to remain ethical and continue to safeguard sensitive client data.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Elevating Cyber Risk Analysis During M&A Due Diligence

Before a deal closes on a merger or acquisition, due diligence investigation will ensue to confirm goal alignment and identify any obstacles present. There are several integral components of this process such as identifying transaction purpose, legal obstacles, financials, sale history, and technology usage. Cybersecurity has always been on the list, however, now more than ever it is essential to perform inquiries into cyber risk as a separate category of due diligence review and also throughout the life of the transaction. Unlike other investigatory components, teams cannot just review cyber risks once. This instead needs to be a consideration at every stage from strategy through integration.

Every organization with a technology footprint carries a degree of cyber risk, and failure to identify those prior to merging or acquiring another organization can result in disaster. Putting extra effort into cybersecurity review fosters successful, secure transactions and ensures everyone at the table is comfortable or has the opportunity to tailor strategy before it is too late. This is especially true during the due diligence phase to identify overlooked cyber risks earlier on in the timeline.

Five essential considerations for elevating cyber risk evaluation during the due diligence process.

- **Collaborative approach:** Create a playbook outlining roles for key stakeholders and who should come to the table at each phase. Having legal counsel direct matters from the beginning of a transaction is beneficial because it provides a layer of privilege protection that can carry forward through due diligence inquiries. Going in with a collaborative mindset not only supports goal achievement for all interested parties, but also offers an opportunity for cyber professionals to have a larger presence throughout the life of the transaction. Developing strategy with "security by design" will help align expectations and ensure that cyber risks are at the forefront of due diligence investigations so teams can identify gaps and react accordingly.

- **Heightened risk factors:** Many are not aware that threat actors watch for talk of M&A activity and view this as

a time when security awareness falls, thus leaving an organization more vulnerable. This increases the likelihood of ransomware attacks, phishing, and other attempts to access sensitive or proprietary information. Besides the nature of the transaction heightening risk automatically, it is also crucial to identify data breach history, dark web exposure, supply chain activity, contractual obligations, and pending legal action. Being aware of these factors helps teams understand where risk exists and what action to effectuate in order to avoid compromise or remediate before moving to the next stage of the transaction.

- **Cyber strategies:** Do not forget to take a deep dive into the acquiree's cyber program. Key inquiries include policies around personal device usage and remote working, employee training and onboarding mandates, compliance procedures, CISO presence, incident response approaches, audit frequencies, technology vetting process, and other unique cybersecurity controls. Knowing these things before close of deal will make the transition smoother and help determine what to address in order to maintain uniform security practices. It also lessens the risk of overlooking a major responsibility or gap prior to integration.

- **People and technology:** Cyber risk can increase based on the people and technology that come along with the transaction, so it is crucial to perform due diligence in this regard. Keep apprised of reputation, market presence,

and methodology preferences for the key people coming over. The last is really crucial with technology deployment, as oftentimes people will need certain solutions and processes to continue thriving and contributing in the manner expected after a deal closes. Taking an agnostic approach to technology will help evaluate cyber risk and match current processes to industry best practices. Key stakeholders can discuss assessments, determine risk tolerance, and consider alternative approaches that lessen risk while still advancing goals.

- **Privacy implications:** Consider how privacy fits into cyber risk due diligence, as current and future legislation around the globe will continue to influence the level of cybersecurity needed to protect sensitive information. Factors to include in exposure review include applicable laws, global presence, personal data storage, and compliance efforts. Discounting this step and similar obligations such as contractual mandates can result in legal exposure after the deal closes.

Incorporating the above into cyber risk analysis during M&A transactions will enable organizations to better manage risk and make informed business decisions. This requires having collaboration between several key actors including legal, stakeholders, IT, and human resources. Remember that each review will have unique characteristics, which makes proactive cyber screening before jumping into a transaction a crucial asset. Adding internal IT and security professionals or outside consultants to the risk management process is one way to ensure thorough cyber risk due diligence ensues. This will facilitate any changes or discussions needed prior to closing a transaction and guide cyber initiatives after the two organizations become one.

To hear more about this topic, consider listening to our podcast, Cyberside Chats.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

International Data Transfers: Knowing Which Rules Apply to Comply

While countries all over the globe continue to make data privacy strides, comparing similarities and differences between the EU and U.K. is important in light of Brexit. It is also crucial to know the differences as they impact transfers with the U.S. Analysts and affected organizations have been watching to see how Brexit will influence data privacy regulation in the U.K., and this year some significant changes have materialized. It is important to understand which transfer mechanisms are available to export data from the EU member states and the U.K. to other countries. Also, to monitor any privacy developments that could influence the current adequacy decision allowing data to flow freely between the U.K. and EU member states.

EU Transfer Updates

Due to the landmark Schrems II decision that came down in 2020, the European Commission created new standard contractual clauses (SCCs) last year applying to personal data transfers from EU member states to other countries. These are inapplicable for transfers involving the U.K. because of Brexit. The new SCCs enhance accountability and transparency to ensure transfers to countries with privacy standards deemed inadequate align with General Data Protection Regulation (GDPR) standards.

Recently, the EU reached an agreement in principle with the U.S. on another mechanism to effectuate cross-border data transfers. The Schrems II ruling invalidated the prior Privacy Shield framework, and the EU does not recognize the U.S. as having adequate data privacy laws or safeguards. In the absence of a new framework, only the new SCCs were available to effectuate these transfers. The Trans-Atlantic Data Privacy Framework would offer a streamlined option to complete such transactions and enhance protection over sensitive EU consumer data. Organizations would also be able to self-certify compliance. This is a huge asset for employers operating in multiple countries or organizations targeting consumers across borders that need to transfer data with ease. Here are some key details that have been released to the public thus far:

- U.S. intelligence agencies will only be able to access data in limited situations when needed to protect national security.
- There will be increased oversight and review over data transfers.
- There will be a review court for EU residents to turn to with non-compliance issues.

While organizations should anticipate this framework, until there is a formal agreement nothing is certain. However, there has been chatter that the framework could become official sometime this year. Interested parties should also monitor whether the EU creates a similar framework with other countries deemed inadequate under the GDPR and any transfer mechanism trends that emerge.

UK Transfer Updates

This February, the Information Commissioner's Office (ICO) announced new SCCs available for U.K. data transfers. Prior to this, the U.K. was in limbo due to Brexit and relied on adapted versions of the old EU transfer clauses for international data transfers. The new U.K. clauses are more in line with the nation's vision for data privacy protections, which is starting to

materialize with a pending data reform bill that would reduce compliance obligations and reform how ICO operates. If reform occurs, the EU-U.K. adequacy decision may be deemed invalid, so it is critical to monitor this bill.

The new U.K. SCCs are comprised of an international data transfer agreement (IDTA) and addendum accounting for both new agreements and those already including EU clauses.

- **IDTA:** Parties can insert this clause into current commercial contracts or create a separate supplementary agreement. Similar to the EU clauses, IDTA accounts for Schrems II concerns and requires data exporters to perform risk assessments. However, there are notable divergences including an option for arbitration, no regulation over audits, absence of a modular structure, and the ability to integrate terms from a prior linked agreement. With controller to processor transfers, gaps exist requiring an additional data processing agreement to remain compliant.
- **Addendum:** This applies when a contract already contains an EU model clause. To cover what is needed for U.K. data transfers, the parties would simply have to add the model addendum to the existing agreement.

In March, these clauses became effective but there is still time to comply. All new contracts signed after Sept. 21, 2022 must use these clauses. For existing contracts, old data transfer clauses need to be replaced by March 21, 2024. The ICO also provided guidance on preventing ransomware including several scenarios aimed at risk mitigation that organizations can use during tabletop exercises. The ICO is expected to announce further guidance on topics such as IDTA use, impact assessments, and more. Affected organizations need to review IDTA, the Addendum, and any guidance to inform necessary compliance updates and anticipate the ICO's approach to enforcement.

Conclusion

It is common for organizations to have a global presence or the need to conduct activities outside their borders. To avoid delays and penalties that affect operations and industry reputation, keeping up with data transfer specifications must be a top priority. While the EU and U.K. are major players to keep informed of – especially for U.S. organizations – it is critical to know the data privacy laws for all countries involved in a transaction. This promotes better compliance habits in such a dynamic landscape and will help shine light on gaps requiring attention.

If you enjoyed this blog, consider reading Predicted Implications of the EU's Digital Markets Act.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

How to Handle Privilege When Producing Documents to the Government in Antitrust Matters

The identification of privileged content remains one of the most time-intensive undertakings of any discovery project. In recent years, there have been significant developments in the ability to use analytics tools and artificial intelligence (AI) to identify the existence of privilege. This helps legal teams streamline the review process while maintaining privilege.

Below is an outline of steps to consider for handling the identification and review of potentially privileged content in antitrust matters. Utilizing advanced tools and following the appropriate steps can be a big time-saver when producing documents to the government during an antitrust enforcement action.

Step One: Compiling a Privilege Screen

The legal team (corporate and outside counsel) and the data provider should work closely to compile a "privilege screen" of attorney names and terms that can signify the existence of privileged data. The privilege search term report will show the total and unique number of "hits" for each name and term. Once the screen has been finalized, it is run against the data that is possibly responsive. As with any search term analysis, it is important to test the results of those search terms, particularly terms that could have more broad usage and may be generating false positives.

Step Two: Highlighting Terms Indicating Privilege

All "hits" are then highlighted in the review database. The team can also deploy custom analytics workflows to identify documents and document families that only have privilege terms appearing in the footers of emails, as it is often customary practice to include the "privileged and confidential" disclaimer on all emails.

Step Three: Deploying an AI Model

To reduce the number of false hits and expand the scope to include privileged documents the privileged terms might miss, counsel can also use analytics and AI tools to supplement the standard privilege screen. This starts with feeding sample coded documents into an AI system. These systems typically use the text and metadata of documents to score each on a scale from 0 to 100 – the higher the score, the more likely the document is privileged. The scores provide another means of identifying privileged documents and help to reduce the number of false hits returned by the standard privilege screen.

A privilege expert (typically from the review provider) can then train the system using examples from the collection. The training effort is typically less than 3,000 documents and continues while the system is gaining reasonable value from additional training. The expert also uses social network analysis, domain analysis, and other analytics tools to identify potential privilege actors. Statistical sampling and targeted searches of the null set are then used to validate the results of the privilege AI model.

Step Four: Sorting the Documents

After deploying the AI model, documents identified as possibly privileged are sorted into two groups:

- **Higher Probability Documents** are those containing certain attributes that typically signal the existence of privileged content. Common examples include communications with outside legal counsel for the end client and communications with internal counsel. These documents can be moved directly to a privilege log review and redaction workflow, which obviates the need for first-level privilege review. The reviewer conducting the privilege log review will then confirm the existence of privilege.
- **Lower Probability Documents** are those that have some indicia of privileged content, but still require validation through the first-level review process to confirm the existence of privilege. Outside counsel will decide whether to review all of the documents flagged as potentially privileged or to cut off review for those with lower probability scores.

Step Five: Identifying Additional Privilege Sources

Once the review starts, the team will identify additional names of individuals or organizations that may create or break privilege. New privilege names are escalated to outside counsel to determine whether they need to be added to a privilege search term report. Any new names added to the privilege search term report will then be normalized across previously reviewed, non-privileged documents.

Conclusion

The combination of traditional and rigorous screening with AI privilege tools will provide the best results when reviewing for privilege in antitrust matters. Additionally, the process involved is defensible. Counsel can easily explain the process above to a regulator who questions methodology. Coupled with the protection of a protective order regarding the inadvertent production of privileged material, this provides a thorough workflow for identifying and properly logging privileged data.

This blog post is derived from the Chapter titled "Outsourced Document Review: Data Intelligence, Technologist Lawyers, Advocacy Support" by Edward Burke and Allison Dunham, which appears in the Thomson Reuters treatise eDiscovery for Corporate Counsel (2022). Reprinted with permission, © 2022, Thomson Reuters. Jason Butler also contributed to this blog.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Intellectual Property Business Management (IPBM) Evolves

Like other legal operations functions, today's Intellectual Property Business Management (IPBM) model focuses on business impact. The IPBM model has shifted away from managing IP with a purely legal or asset-based perspective to a focus on the impact of an organization's IP portfolio on the business, and vice versa.

In essence, IPBM is shifting from an IP prosecution-based lifecycle to a business-integrated lifecycle. The overarching objective of IPBM is the support of core business operations, revenue generation, and corporate value with a robust data-driven decision-making program.

Legal, Operational, and Business Alignment

The point of implementing an IPBM model is to broaden an IP operation's capabilities to align strategy, process, and organizational dynamics. This model relies heavily on involving a greater number of departments and decision-makers in the analysis of how to turn that insight into strategic action.

The illustrative model for IP Business Management below describes the central role IPBM plays in addressing core asset management challenges to drive positive outcomes. As the model portrays, the central tenet of IPBM is the integration and alignment of the organization's legal, operational, and business processes to identify, address, mitigate and resolve the challenges of IP management.

IPBM for corporations: An Illustrative Model

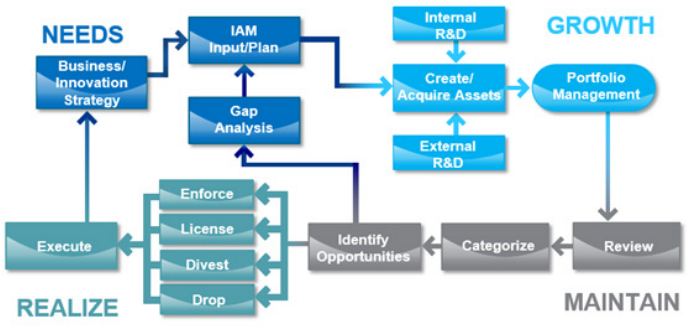
IPBM, thus, presents a unique set of opportunities to increase value to the corporation through better innovation and risk management, while deriving more revenue and cost savings. From a more tactical perspective, IPBM aligns core organizational competencies and then delivers efficiencies by defining, monitoring, and supporting everyday processes that capture, nurture, and manage the organization's innovation assets.

In this context, the integration and alignment of the organization's legal, operational, and business processes provides insight into an IP organization's activities – enabling IP leaders to have informed discussions with their business peers

and make decisions about where to best invest organizational resources. Among the goals is a clearer understanding of how the activities of one set of stakeholders could—or should—affect the outcomes of another set of stakeholders.

IPM as a Continuous Business Process

To further explore this concept, the flow chart below represents the integrated business process loop defined by four phases: Needs, Growth, Maintain and Realize. This flow chart shows the progression from traditional IPM, which largely focused on—and was limited to—innovation management and IP prosecution (the "Growth" phase in the chart below) to a more dynamic, interactive means of strategic business management. As such, the IPBM Lifecycle demonstrates the importance of aligning business and strategic objectives in the inputs (Needs), the outputs (Growth), and commercialization of innovation.



IPM as a Continuous Business Process—A Lifecycle

The Needs component is where decisions that drive the IP lifecycle intersect with the businesses that drive creation, and where decisions driving business-related outcomes are made. We can refer to this dynamic colloquially as the "businessification of law," where IPBM is dynamic and evolutionary by design.

In the next installment in this series, we will discuss evolving practices in capturing and nurturing innovation.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Remaining Compliant Amidst Challenges When Using Chat Applications in the Workplace

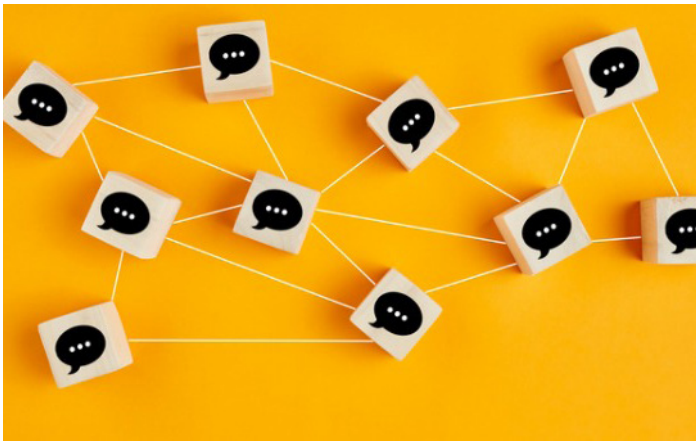
Communication is different in the modern workplace. Gone are the days of phone calls and email being the primary channels of interaction. Many organizations are frequently utilizing chat applications like Microsoft Teams for internal communication. This includes informal chats, formal project discussions, video meetings, phone calls, and group collaboration. User-friendly chat applications are a great way to improve collaboration efforts and streamline projects – especially in a work environment involving remote employees or global offices. However, this also creates new eDiscovery and compliance obstacles to consider when it comes to creating policies around chat application usage and data collection workflows. Not only is business data stored in several cloud repositories, but it is also subject to rapidly evolving global regulations.

Failure to understand where internal data lives and implement appropriate retention protocols can result in violation of regulatory and industry requirements. Consider the four tips discussed below to help meet eDiscovery, human resources, and other compliance obligations.

#1) Remain aware of communication habits and where data may live internally

This is arguably the most important step because lack of visibility is now a common issue. Data usage is complex and moving outside of the traditional singular instances of IT storage locations. Data in modern communication platforms is stored in many locations across the enterprise. Not being aware of where sensitive information resides can cause major compliance issues resulting in regulatory fines or increased litigation costs. Leadership cannot ignore the fact that workplace communication preferences have changed and will continue to evolve as new technologies enter the market.

Since chat applications are here to stay, it is crucial to understand how these solutions store data. For example, there are two types of data sources in Teams (chat and channel), which adds complexity to collection and review. Teams' chats are automatically stored in a user's online mailbox. The files shared in Teams chats are stored in the sender's OneDrive for Business site. Pulling all this data back together as one



conversation thread becomes challenging during the review process.

Channels are harder to piece together because there are multiple people with access—some of whom do not even participate in the conversations or get left on after project completion. To add further complexity, the chat is stored in a dedicated group mailbox and the files sent are stored in a dedicated SharePoint site. When private channels are in use, the chat is stored in the end user's mailbox and the files sent are stored in another SharePoint site. This renders identification a challenging feat. A hybrid approach using technology and custodian interviews is an optimal way to determine which channel conversations to attribute to a certain person and where relevant data resides. It is also crucial to remember private channels can be a data source for collection or legal holds.

File sharing in modern chat applications is difficult not only because of the complex storage strategy but also because of versioning. With Teams, it is the default setting for SharePoint and OneDrive to save the last 500 versions of a file. This version history is not based on intentional actions the user takes but rather on saving incremental versions. This means many versions of each file will exist. Matching a chat to the time a file was sent is crucial to maintain context during review. Failure to do so can result in reviewing a subsequent version of the

file consisting of different content than what was originally provided. Exploring solutions that can piece conversations back together and preserve context can relieve review burdens associated with modern chat data.

#2) Update data governance workflows

Data is at an unprecedented level and will only continue to grow. This requires a deep understanding of how frequently utilized applications generate data and where retention gaps exist. Organizations need capabilities around deleting unnecessary chat data. Platforms such as Teams already offer this as a built-in feature. Carefully determine what the retention period should be for chat data and whether to store certain communications longer than others. Having sound retention policies in place is a great way to reduce risk while also minimizing the data review pool for future cases or investigations. Other solutions that promote compliance include label analytics and rich audit trails. After implementing a sound retention policy, consider creating an equally thorough in-place preservation practice to comply with legal and regulatory requirements.

#3) Implement privacy and data protection management controls

Investing in data privacy management tools must be a top priority as more governing bodies continue to update their privacy laws to provide consumers with enhanced protection. It is now the norm for employees to discuss customer matters and share sensitive information via chat applications. Additionally, having a data loss protection solution in place can greatly minimize data leakage risk and allow organizations to remain compliant with applicable privacy regulations. Another offering to explore is deploying automatic policy alerts when a user violates pre-established regulatory or corporate communication policies.

#4) Enhance forensic auditing and investigation capabilities

Opting for extended auditing logs is a way to improve forensic auditing and investigation. This will include extended licensing. It is crucial to have solid lines of communication between IT, legal, and leadership to understand current licensing capabilities. This helps legal and compliance teams to know where to advocate for additional services that can offer business value. Advanced auditing solutions preserve communication logs longer, offer extended retention options, and provide deeper visibility into messaging activities such as message read features or edited chats.

When it comes to data retrieval needed for a case or investigation, organizations need to know how certain data is structured to collect it effectively. Being aware of common obstacles presented with chat data will shine light on the solutions needed to remain compliant. Examples include modern attachments, reactions, versioning, gifs, emojis, and stickers. All of these unique data sources exist within applications like Teams but are stored and shared differently. A service provider with capabilities around collecting and transforming complex data is an optimal outsourcing opportunity to better manage these processes.

Conclusion

To continue to meet legal, business, and regulatory compliance challenges in the modern workplace, the ability to protect and quickly retrieve vital information is necessary. Integrating the considerations listed above into eDiscovery and compliance workflows can help organizations remain compliant. The goal should be to implement tools and partnerships that relieve the data management and collection burdens inherent in emerging technologies.

If you enjoyed this blog, consider viewing our recent webcast Emerging E-Discovery and Compliance Considerations in a Microsoft Teams-Centric Modern Workplace.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

IPBM Evolves: Innovation Goes Social

Having described the modern Intellectual Property Business Management (IPBM) model in our prior post, we now focus on a key driver in the shift toward IPBM - the challenge of cultivating and protecting innovation. Nurturing the participation of inventors and IP asset developers is paramount in this movement. Increasingly, the leading IPM systems vendors have sought to develop new tools to better engage and empower all stakeholders in the innovation lifecycle. Many of the advanced solutions covered in the 2022 Hyperion Intellectual Property Management MarketView™ report have introduced new and improved tools to drive invention disclosure, information disclosure (IDS) and prior art searching processes.

Inviting more people to the party

This is partly a result of better understanding of user personas. In the IPBM model, attorneys, inventors, and business executives play important roles in the innovation lifecycle. Despite a historical focus on the docketers and paralegals who handle data entry, vendors are now addressing the needs of the lifecycle's upstream and downstream stakeholders. IPBM advances "innovation in context" and newly developed tools invite users into a harmonized information management process for better outcomes.

The value of sophisticated innovation management is derived from the deliberate involvement of multidisciplinary stakeholders, whether R&D specialists, scientists, engineers, business managers, marketing managers or C-suite executives. Innovation management is necessarily broad -- inclusive of patentable technology, protectable trademarks, copyright protected content, vital trade secrets and institutional know-how that strengthen an organization's ability to compete. And there is tremendous business value through involvement of multidisciplinary stakeholders which arms decision-makers with the ability to contemplate the potential business impact of innovation. [More on capturing data in a later post in this series]

Making sure all voices are heard

Improving the tools that connect stakeholders, including law firms and other outside providers, is another element driving innovation management in an IPBM paradigm. Collaboration tools – hardly a new idea – have long failed to deliver any real collaboration, often settling for an online document repository (typically manually maintained and woefully out-of-date). However, IPBM addresses the root cause of legacy collaboration failures with a focus on 1) incorporating cross-disciplinary lifecycle participation, and 2) integration and alignment of workflows.

IPBM is not a "collaboration portal;" rather, it is a paradigm designed from the ground up to involve stakeholders when and as they are needed in the process (both as active participants and passive monitors), with audience-specific information. This new approach can be seen in emerging vendor efforts to provide tools that not only capture and protect innovation, but also encourage it through social media-like extensions of their platforms.

In the future, inventors will more easily work as a community, not only collaborating on new ideas, but also leveraging crowd-sourcing concepts to facilitate awareness and promote winning ideas within this extremely important and historically underserved user community.

The unifying technology framework that underpins IPBM will be discussed in the next installment of this series.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Canada's Long Awaited Privacy Bill Introduced: How Does it Stack Up?

There has been chatter in Canada for nearly two years about initiating comprehensive legislative reform to the country's data privacy landscape. The process recently ramped up this June with the introduction of a bill to pass the Digital Charter Implementation Act. This is a comprehensive law that would not only enact a new data privacy law (referred to as the Consumer Privacy Protection Act/CPPA), but also laws to create a data protection tribunal and regulate artificial intelligence (AI) development. The bill is expected to remain pending for the next year or two, as it needs to go through the remainder of the legislative process and then is subject to a waiting period so organizations can create compliance initiatives. If passed as proposed it would join the ranks of the GDPR with some stricter provisions and heavy fines, so it is important to monitor the process and start preparing now.

The Old Law

Canada has relied on the Personal Information Protection and Electronic Documents Act (PIPEDA) to regulate data privacy for over twenty years. In that time, the world has changed drastically in terms of electronic communication and data exchanges. Almost everything is digital now, which renders PIPEDA extremely outdated and places Canadian consumer data at risk. The major gaps that exist under PIPEDA yield greater opportunity for data misuse and heightened breach risk. This includes the absence of enhanced consumer control – like a firm right to deletion – and lack of oversight requirements to eliminate unnecessary processing or prolonged storage of personal data.

The New Law

If the Digital Charter Implementation Act passes, the CPPA would effectively replace PIPEDA and provide Canadian consumers with more control over their data. The law applies to data processing at a federal level, which is needed as some provinces like Quebec have already modernized their privacy landscape. Having a federal standard will provide clearer guidance for organizations operating in multiple jurisdictions and also serve as a model for future provinces wishing to create their own legislation.

In addition to data processing surrounding commercial activities, the law also applies to data processed for federal employees or job applicants. Employee data in the private sector is not specifically delineated, which tends to be the norm with other privacy laws around the globe.

Here are some important CPPA provisions to note:

Consumers

- Key consumer rights include erasure, access, disposal, correction, and portability. These rights generally appear in the majority of new data privacy laws.
- Individual consent is required before an organization can lawfully collect data. Exceptions include data processing activities for the following purposes: public interests such as a health emergency; publicly available information; anonymized personal information; investigating a breached agreement under federal law, provincial law, or security safeguards; when it would be reasonable to assume that information is being collected for business purposes; and to a service provider when equal protection is established, which is often via contract. These exceptions are meant to provide a better balance between consumer rights and an organization's interests in using the data. This list is not exhaustive.

Organizations

Before collecting data, organizations must determine and record the purpose. Weighing interests with consumer rights is part of this process, which is similar to the GDPR's impact assessments.

- Organizations must designate a single individual or team to oversee compliance efforts. If organizations already have a data protection officer appointed for GDPR compliance, obligations will undoubtedly overlap.
- Organizations must create a privacy management program accounting for all CPPA obligations. If there is already one in place, the compliance team needs to prepare an audit in order to identify any policy or process gaps. For example, the CPPA clearly directs subjects to delete personal data once the use purpose is fulfilled. This may require changes to existing retention programs.
- The ability to collect and process data for minors will be limited, as the CPPA clearly classifies this information as sensitive. This was highly debated in the bill's previous version.

Penalties and Enforcement

Allotted penalties will be the greater of the following amounts: five percent of an organization's gross global revenue or 25 million CAD for criminal or egregious offenses; three percent or 10 million CAD for administrative ones. This is significant, as the top fines allotted under the GDPR are lower. The data protection tribunal will be able to hear appeals regarding fines that the Privacy Commissioner issues.

The Privacy Commissioner can also issue compliance orders, mandate third-party audits, approve internal certification programs, and compel information sharing with other regulatory bodies when appropriate.

It is important to account for the AI component of the Digital Charter Implementation Act, as this seems to be a trending concern. If passed, among other things this law would require operators of high impact AI systems to mitigate risk associated with bias and accelerate transparency with the public. There will be a list of prohibited conduct and a separate commissioner to conduct enforcement. The EU and UK also have proposed laws relating to certain AI regulation, so it will be interesting to see the differences as laws pass in different areas of the world.

Final Thoughts

The protections outlined above illustrate how the new Canadian law aims to strike a balance between business interests and consumer rights, while still paralleling strict protections under laws like the GDPR. As it continues to move through the legislative process, monitor any amendments or interpretive guidance. How the penalty system plays out will be particularly interesting, as there could be record-breaking fines. Remaining informed will help organizations proactively create compliance roadmaps and be better prepared when the law becomes effective. Finally, make sure to obtain legal advice before making any decisions.

To learn more about how Epiq can help you, click here.

Visit blog post on the Epiq Angle

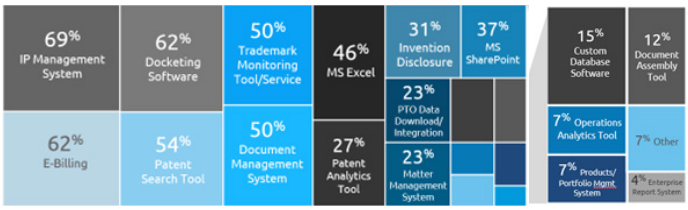
The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

IPBM: The Unifying Framework Behind IP Management

The first two installments in this series explained the evolution of the Intellectual Property Business Management (IPBM) model, noting that it is not a platform or "collaboration portal," but rather a paradigm designed from the ground up to engage stakeholders when they are needed in the IP management process. IPBM is driven by the technologies that support legal operations and performance.

Hyperion benchmarking data shown below demonstrates that an IPM system alone does not address the breadth of needs of an IP organization.

Technologies Used to Manage IP Assets



While 69 percent of IP practices leverage an IPM system, and another 62 percent use traditional docketing software, we are surprised by the breadth and diversity of other tools the market leans on to marshal data and drive decisions. E-Billing software, central to outside counsel participation, is as prevalent as Docketing software. The market is clearly manifesting a need for an array of tools to capture, nurture, manage, protect, and defend intellectual assets. Yet organizations overwhelmingly address these needs with a "whack-a-mole" approach, acquiring technology to address a specific, narrow need when a challenge arises.

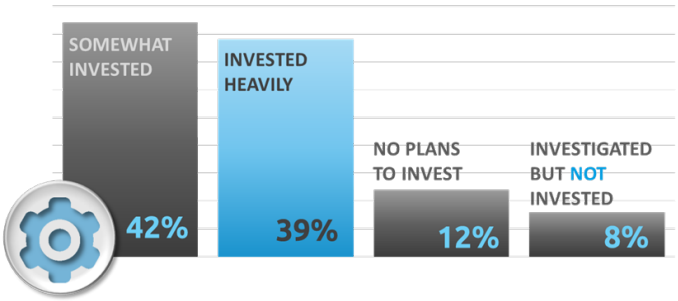
However, help is on the way! IPBM can present a unifying framework that allows organizations to understand their holistic information management needs and address them in a cross-functional manner. IPBM combines innovation, legal and business information to provide powerful insights into the complex relationships that exist between these departments. This model provides inputs for the elusive ROI assessment on which both business and IP leaders depend to make investment trade-off decisions.

In addition to the range of tools employed in end-to-end IP lifecycle management, a trend among leading IPM vendors examined in the 2022 Hyperion Intellectual Property Management MarketView™ report is the diversification and sophistication of capabilities in the IPM system itself, which provides clients with access to the widest range of functionality possible. One notable example is Anaqua's integration of AcclaimIP's patent search engine technology into Anaqua's AQX software, a solution-set that is not only compelling but also directly addresses the 54 percent of the market that uses patent search tools as essential technologies.

Leveraging Workflow & Automation Tools

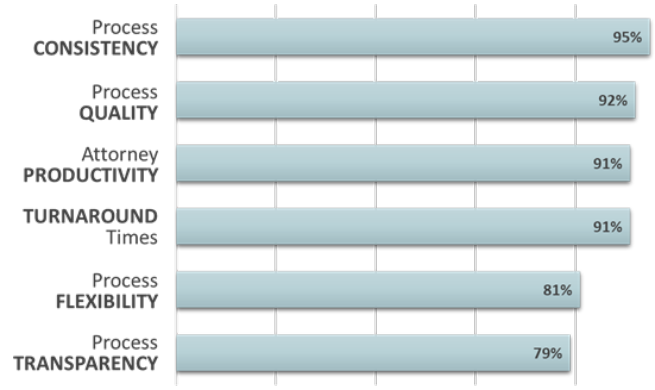
IP organizations are actively investing in workflow and automation tools in the form of both integrated IPM point systems [integration of workflow technology is covered throughout the reportl], and standalone Business Process Management tools for administrative workflow, such as invoice approval, as well as practice-based task management, including automated and specialized docket entry. As shown below, most of the market has invested in workflow and automation tools to support operations. Nearly two in five IP organizations characterize their investment in workflow and automation as "heavy,". Adoption of process automation is deeply ingrained in the market with more than 80 percent of organizations having invested in some workflow and automation tools.

IPM Investment in Workflow and Automation



The graph below shows the drivers in workflow investments. Sentiments are strong and unequivocal, with Process Quality, Consistency and Productivity reported as the highest (and statistically significant) drivers.

The Drivers for Investment in Workflow and Automation



Collectively, these categories can be summed up in a single word: efficiency. Efficiency, in the IPBM context, heavily rests on "operationalizing insight," and the stated goal of broadening an IP operation's capabilities to align strategy, process, and organizational dynamics. Hence, a connection is drawn between the next-generation IPBM paradigm and the incorporation of tight, succinctly defined uses of workflow and automation.

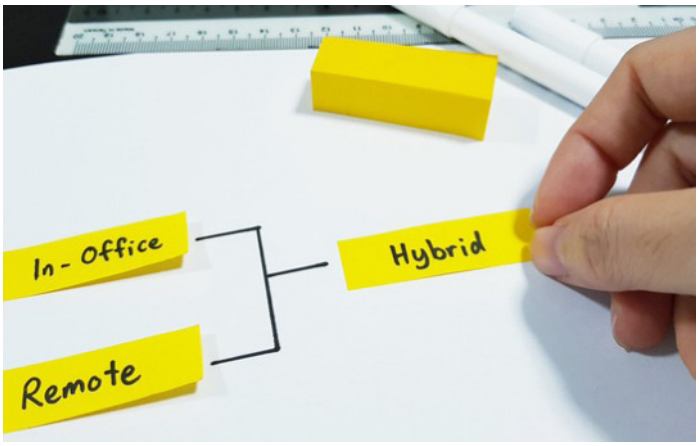
In the next installment of this series, we will focus on using metrics for operational success.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Supporting the Hybrid Work Environment: Three Market Trends

The business world has changed drastically over recent years. A hybrid work model is now the new norm – especially in corporate settings. The virtual trend is even emerging in industries such as legal and healthcare which have been traditionally and exclusively in-person. Such widespread change creates opportunity for organizations to transform operations, unlock transformation, and maximize technology usage. Such transformation is necessary to continue successful operations, maintain revenue streams, and create a positive company culture accounting for varying working styles. Being cognizant of technology and outsourcing trends will help organizations decide the best route to effectuate meaningful change. Here are three emerging trends to monitor that support hybrid working models.



1. Leaders are reimagining the role of the physical office.
    - For many corporations, employees are working remotely full-time or on regular schedules. With fewer people coming into physical offices, operations leaders are having to reimagine and strategize what the space should look like to accommodate working trends. Factors to evaluate include employee schedules, remote policies, and the purposes for working onsite. Moving away from the traditional office model can look like increasing shared spaces, downsizing, or eliminating the physical office altogether. This leaves operational gaps that leaders must address in their hybrid programs and outsourcing budgets. All of these factors will fuel the vision for an innovative office model that promotes effective collaboration and accounts for current company culture.
2. Industries historically resistant to change are accelerating transformation efforts.
    - Before the pandemic, hybrid work models were available, but they were generally limited to industries known for early tech innovation or organizations trying to get ahead of the curve. Now, virtual offerings are everywhere – even in unanticipated settings like a law firm. The pandemic forced people to realize the benefits of virtual offices and tools, resulting in a focus on how to be more effective and efficient through intentional investments. This is a significant historical shift that will permanently change the way people work across the globe and render it easier to embrace change in the future.
3. Organizations are being more intentional with outsourcing.
    - Successful transformation during a time of change requires an approach that improves processes and increases productivity. How this is achieved will look different for every organization and should evolve alongside progressive goals and company culture. Oftentimes, outside partners are an efficient and cost-effective way to carefully craft the right strategy and then achieve said goals. A service provider can leverage expertise to pinpoint where change is needed and implement optimal solutions. In a hybrid environment, it often makes sense to outsource certain functions previously not considered. For example, many organizations have prioritized outsourcing digital mailrooms, document processing, AP/AR Billing, and administrative functions. While it is not a new concept to move these functions outside the enterprise, it is becoming more commonplace in the hybrid work environment as the role of the physical office changes.

Conclusion

The shift to hybrid work requires leaders to be creative and bold so that they can focus on which tools and processes will foster efficient and effective operations. Being aware of market trends and what employees need to foster efficiency when working remotely will help create successful and sustainable hybrid programs. As the hybrid work model continues to evolve, organizations should continue to keep tabs on alternate approaches, innovation occurring in industries relevant to their operations, and compelling outsourcing opportunities.

If you enjoyed this blog, consider reading our whitepaper called How the Hybrid Work Environment Unlocks Business Transformation Opportunities.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

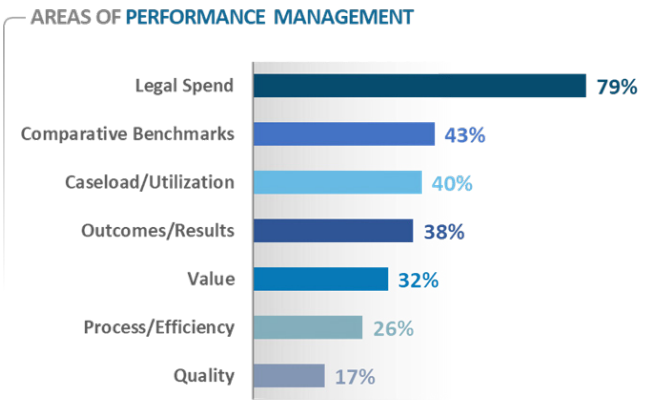
IPBM Decision Support: Using Metrics For Operational Success

A key component of IP operational maturity that we have been describing in this series is the recognition of the vital role data plays in operational success. Today's business environment demands high performance while consistently reducing costs. The use of data to enable the general counsel and chief IP counsel to make informed and timely decisions is essential. The creation of quality data streams, appropriate data models, and the use of visualizations provide the vivid, actionable intelligence that executives need.

What began as buzz has exploded into near-universal demand. At the heart of the surge is the use of Key Performance Indicators (KPIs), providing stakeholders with real-time insight into current activities and informing strategy adjustments in the management of intellectual property portfolios. As we often say, you can't master what you don't measure. Mastery comes from careful planning and collaborative discussion at the front end of developing an analytics program. Not surprisingly, recent Hyperion benchmarking reveals that most organizations have introduced a handful of KPIs or have launched full-fledged decision-support analytics programs.

The appetite for data-driven decision-making by law departments has resulted in metrics that cover value, process/efficiency, outcomes/results, and comparative benchmarks—extending far beyond spend and budgeting.

Performance Metrics

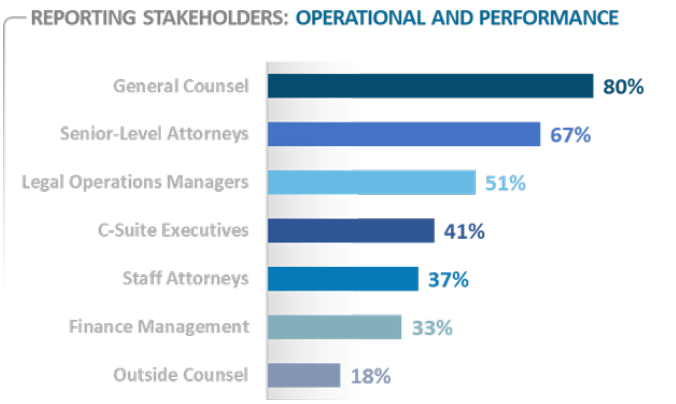


In the quest for operational maturity, organizations have begun to pinpoint strategies that propel value and create KPIs that support those strategies. The figure below demonstrates how KPIs can reflect organizational values and serve as actionable intelligence for both defining performance and measuring success. KPIs enable IP leaders to have informed discussions with their business peers and make decisions about where to best invest organizational resources.

Understanding the Drivers of Value in IPBM

Not only has the breadth of KPIs expanded, but so has the audience. It is not just the general counsel, chief IP counsel and senior attorneys consuming IP KPIs for spend and outside counsel management—the traditional reporting lines—but our benchmarking shows high levels of stakeholder involvement across functions. Legal performance management rarely involves a single, insular constituency, and operationally mature departments understand the collaborative power of a diverse audience.

Performance Reporting – Diverse Stakeholders



Even as the creation and utilization of KPIs and related metrics continue to grow rapidly, this is still a developing discipline. Obstacles to quality reporting still exist, with roughly half of respondents attributing these challenges to a lack of tools, metrics, or data. This finding is wholly consistent with the lackluster use of technology discussed earlier in this series and offers color to the story of frustration with technology in today's market.

Major Obstacles to Measuring Performance

The next and final installment in this series will provide our analysis of the evolution of outsourcing services and practices

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

2022 eDiscovery Update

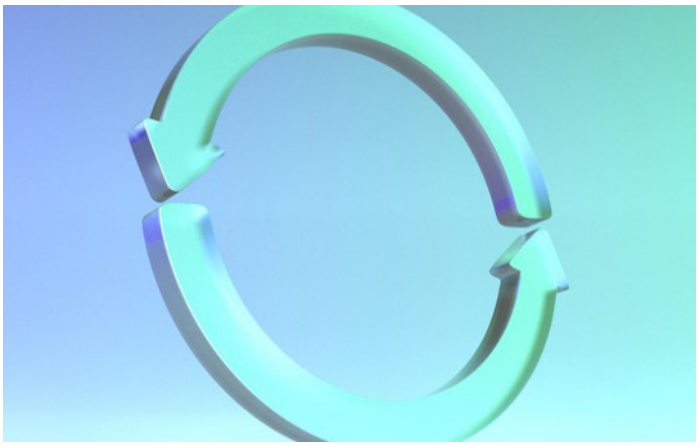
The world of eDiscovery is constantly evolving in the face of new tech trends and legal innovation. This often introduces new collection, preservation, and production challenges that require further analysis and updated best practices. It is important for litigators and other eDiscovery professionals to follow new eDiscovery trends, rules, and court interpretations. Here are four recent developments that eDiscovery practitioners should monitor, as they will likely influence practice, legislation, and case law around the country.

#1: Crafting eDiscovery Requests with Reasonable Particularity

Earlier this year, the Sedona Conference published the "Primer on Crafting eDiscovery Requests with Reasonable Particularity." This is not a new concept, as Rule 34 has required parties to draft production requests with reasonable particularity since 1970. This is not a one-size-fits-all requirement as it is very fact specific. In 2015, amendments became effective seeking proportionality and specificity with discovery requests. However, there is lack of legislative guidance on what constitutes "reasonable particularity," and the courts have still been experiencing an influx of vague and overbroad requests that result in unnecessary case delays and increased costs.

With new ESI sources constantly emerging, vague, and overbroad requests can be very burdensome and may result in data dumps where a lot of produced information is not relevant to the case. Courts have ordered parties to amend requests asking for things like "all communications" to avoid this. The Sedona Conference released the primer on this topic to help practitioners comply with the rules and harmonize the case law out there, as modern eDiscovery can complicate this feat. Here are some key practice considerations from the primer to guide attorneys crafting discovery requests with reasonable particularity:

- Determine the specific information needed to ultimately overcome a claim or defense and anticipate likely objections
- Talk to clients and research public resources to obtain preliminary information that can narrow requests



- Hold a meet-and-confer conference with opposing counsel to limit the scope of discovery
- Start by sending a few targeted requests that will hopefully produce documents that counsel can use to tailor additional requests
- Keep costs in mind for both parties
- Set time limits when making broad requests
- Avoid form requests
- Limit requests to specific custodians or geographical locations

Following this guidance should help litigators craft more purposeful discovery requests, thus decreasing disputes and associated costs.

#2: The New York Supreme Court Commercial Division Adopts Rules to Align with Modern Law

Most business exchanges are now conducted electronically due to the rise in virtual work and emerging technologies. Organizations across industries have revamped working models to incorporate hybrid or digital first options that streamline daily operations and offer more flexibility. From an

eDiscovery standpoint this adds to the amount of data needed for a case, can make processes more complex, and increases cost. This creates the need for courts to update eDiscovery rules that account for the dynamic eDiscovery atmosphere.

The New York Supreme Court Commercial division has paved the way by simplifying its eDiscovery rules to provide flexibility and simplify instruction with the goal of decreasing motion practice. The court consolidated all rules and added new provisions and advisory guidelines that reflect the realities of modern business. Key aspects of the new rules include the following:

- A proportionality requirement to measure eDiscovery cost vs. matter benefit
- Guidance for reaching early agreements on common eDiscovery dispute
- Encouragement to leverage AI
- Guidance on preserving, collecting, and producing data defensibly from trending emerging technologies
- Discussion of when cost shifting is appropriate
- provision for parties to claw back privileged information they inadvertently disclosed
- Encouragement for parties to consider new and emerging data privacy laws

While not a comprehensive list, this highlights major concerns amongst litigators across the country. The New York rules are expected to simplify and solve many eDiscovery obstacles early on, thus promoting transparency and eliminating some procedural conflicts. This will likely become the venue of choice for many commercial disputes until other courts similarly modernize their rules.

#3: Predicted Implications of Apple's iMessage Recall Update

A recent update from Apple provides the ability to edit or recall iMessages within 15 minutes of sending. While many users will favor this feature, it poses significant eDiscovery obstacles. It is currently unclear if a recalled message will be gone forever or if there will be metadata to access in the event of litigation. Regardless, this adds another layer to custodial interviews and preservation efforts. Here are three things that litigators should consider:

- **Metadata:** If there is no metadata for recalled messages stored on servers for later retrieval, then the evidence is gone. A party may face spoliation claims resulting in detriment to strategy, delays, and increased costs. If metadata exists, litigators will need to dig deeper to determine where it resides and if retrieval requires unique or challenging collection mechanisms.
- **Custodial interviews:** Can include questions about message deletion or editing to aid with collection efforts. It would also be ideal to ask if someone took a screenshot of a message before it was recalled, as this can serve as alternate evidence of the conversation.
- **Case law and other persuasive authorities:** Just as with ephemeral messaging, interpretation by the courts will be crucial and instructive. Courts have sanctioned parties that use ephemeral messaging applications, placing an obligation on litigators to direct clients not to use these platforms as a means to delete potentially relevant communications when litigation is active or on the horizon. Courts will likely apply the same reasoning to recalled and edited messages, so it is best practice to include this in information governance programs, retention policies, and legal hold instruction.

#4 More Practitioners Are Using Cloud-Based eDiscovery

According to Statista, today more than 60% of corporate data lives in the cloud. With so much data already stored in the cloud, corporations seem much more comfortable moving to cloud-based eDiscovery over on-premise solutions. This year seems to be the tipping point where it can be considered a trend, and adoption will likely keep growing.

Corporations are realizing the many benefits and cost savings that come with the use of cloud-based eDiscovery tools. The main benefits are:

- Scalability: The cloud provides flexibility so that teams can turn the computing power on and off easily, which allows legal teams to easily scale up or down based on deadlines.
- Accessibility: As more cases become global in nature and talent becomes more dispersed, having a cloud-based application gives the option of using attorneys around the world as they can easily and securely access data from any location. This allows for the best teams to be assembled since having the team at one location is no longer necessary. Also, using eDiscovery cloud computing allows legal teams the ability to work together on documents and collaborate on projects no matter where they reside.

- Cost: Using cloud-based platforms eliminates the need for capital expenditure into technology, less staff to support the technology, and less storage space, which translates into significant cost savings.

Since there are still many who are hesitant to move their processes to the cloud, it will take some time for this to truly become the standard – but that is where things appear to be heading.

Conclusion

Keeping apprised of eDiscovery trends and court decisions is key to remaining compliant and ethical in a very dynamic field. This can also help attorneys streamline matters by tapping into innovation. The topics discussed above outline the range of eDiscovery issues that can arise – from new court rules to emerging technologies and beyond. While all different, common themes are the focus on utilizing tools that simplify processes and anticipating challenges to avoid obstacles that can be time-consuming and costly.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

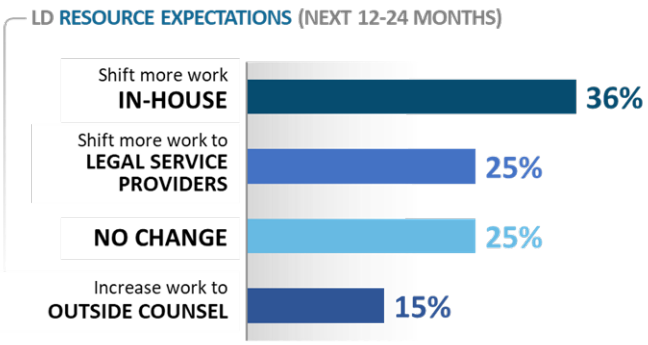
The Rise of Managed IP Services

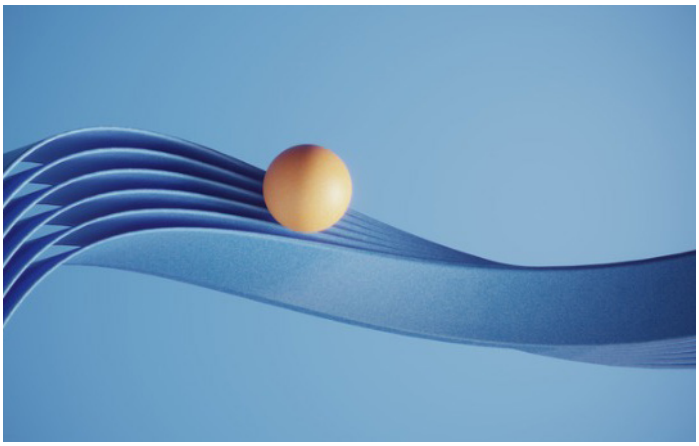
As Chief IP Counsel and in-house legal teams contend with the increasing pressures facing their organizations in the wake of COVID-19, there is an urgent need to rethink legal operations. While the move to digitize and automate the legal function was already underway before the pandemic, it is now a commercial imperative, and the scope and remit is wider than before.

Intellectual property has been at the core of the transformation of legal operations. In addition to the range of tools employed in end-to-end IP lifecycle management tools examined in the 2022 Hyperion Intellectual Property Management MarketView™ report , IP management teams have been the beneficiaries of a diverse arsenal of services that enable them to make better and more thoughtful use of available resources and to extract value from intellectual property assets.

The availability of services and software enable Chief IP Counsels the opportunity to outsource, or to perhaps insource, discrete parts of the IP asset management lifecycle. These decisions require reassessing the balance of resources within an IP organization, which is an ongoing challenge. Decisions will invariably impact the IP department's management of human-capital. This may involve increasing or decreasing headcount, but importantly it is about making better and more thoughtful use of available resources.

The figure below describes how law departments intend to balance their resources during the next 12-24 months.

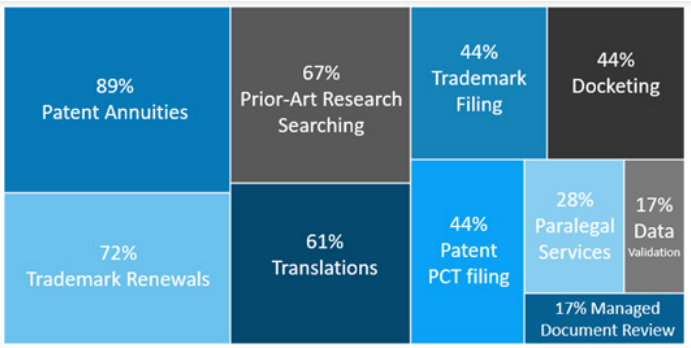




Twenty–five percent of legal departments intend to shift more work to legal service providers. The use of third-party IP services, whether via an LPO model or through more traditional fee-for-service models, is historically most closely associated with patent annuity payment services. However, third-party services have evolved and multiplied. For years now, patent annuity payment services have been critical mainstays of IP Management, as the volume of payments can be both onerous and overwhelming to law firms and corporate IP departments. Patent annuity payments are the oldest solution category in IP and were the catalyst for IP software in the first place.

Now, Chief IP Counsels must evaluate the advantages of trademark renewal services, global patent and trademark filing services, translation services, patent and trademark search services and software, docketing services, document and matter management, contract management, royalty management, anti-counterfeit service providers and an arsenal of analytics tools to support the creation, protection and extraction of value from intellectual property. At the same time, the Chief IP Counsel must manage the global legal work required to manage risk and maximize the value of intellectual property.

| Outsourced IP Services



How does the market now approach the use of IP services vendors for higher-value work? Services such as prior-art research, translations, data validation and data analytics may entail a greater level of competency and sophistication. And therein lies a story. Over the past couple of years, we have seen growing competitiveness from newer, smaller, more disruptive players in the market for IP services. Often, these companies are positioned to offer higher value services at lower costs, as well as integration with their online platform or IP Management system.

Thus, there exists a tension between the traditional model, nurtured by the large annuity service providers, the sophisticated software solutions with parallel services, and the new, innovative offerings of upstarts. How—or whether—to step into the nascent territory of the disrupters is certainly a pressing concern for IP service providers, old and new.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

How Thinking Outside Silos Helps Risk Management and Cyber Threat Response

The term "risk" gets tossed around constantly in the corporate world. But who is responsible for defining and managing risk? This answer is not black and white, as risk type and appetite will look different for every organization. What should be a universal practice is ensuring that all departments understand the enterprise's risk types.

Keeping risk conversations and processes within silos can be dangerous and result in noncompliance. This is particularly important with cybersecurity, as threat actors can penetrate any part of the business. With new attack methods emerging and trends changing frequently, all departments must be aware of what cyber risk the organization has assumed and their respective roles in managing such risk. This requires an effort not to silo risk and have everyone work together to achieve compliance with established frameworks and regulatory constraints.

Interplay Between Risk Appetite and Compliance

Risk can come in many different forms such as reputation, cybersecurity, privacy, financial, legal, personnel, and operations. Compliance risk intertwines with all of these categories. For example, failure to protect sensitive consumer information can result in violation of a privacy regulation or lead to a data breach placing liability on the organization. While each team will be the main actors in defining and managing their own risks, a collaborative approach will help organizations maintain a successful and mature risk management program. Each executive has different perspectives that help reach a balance while still advancing business goals.

Risk appetite refers to what risk level the organization is comfortable undertaking. This can vary depending on the type, company culture, and changing business goals. Factors that can influence decisions on cyber risk appetite include, trending attack methods, type of data the organization collects and stores, industry, geographical location, and the C-Suite's risk tolerance. Even with mature security controls, cyberattacks can happen. When an incident occurs within risk appetite, it is easier to respond as the organization has already accepted

it as a possibility and will have incident response protocols in place. This makes it extremely important for the CISO to work with the C-suite and legal to determine the organization's risk tolerance and communicate this across the enterprise.

Importance of Monitoring Cyber Trends

When it comes to cybersecurity, risk appetite and management efforts can change frequently as new threats emerge. This is an area where breaking the silo mentality is extremely important, as everyone in the enterprise handles data and therefore has responsibility to protect it. Staying on top of new attack methods, competitor compromises, and other cyber data is crucial to receive a real-time view of risk. For example, the Identity Theft Resource Center's "First Half 2022 Data Breach Analysis" report deemed cyberattacks as the most prevalent threat vector ahead of system errors, human mistakes, physical attacks, and supply chain breaks. The top trending cyberattacks are currently phishing, ransomware, and malware. Keeping up to date with periodic reports and comparing trends from year to year or even quarter to quarter can feed into cybersecurity risk strategy.

Understanding the most prevalent risks is important to detect where vulnerabilities exist and the likelihood a certain threat could materialize for a particular organization. This will influence decisions about cyber risk appetite, incident response plans, and necessary controls. There is no way to guarantee that everyone is operating within the organization's

defined risk tolerance without enhanced transparency and collaboration with other departments, including legal. Periodic assessments and enterprise-wide communication on changing protocols relating to cyber risk is a crucial component of risk management efforts. When preparing such assessments, do not forget to account for compliance requirements as what the organization takes on will need to fall within applicable regulatory, client, and internal obligations. While this can be a lot to process, using risk as a way to talk across the silos will help each unit understand what is tolerated and applicable responsibilities to stay compliant.

Best Practices

When – not if – a cyber incident occurs, compliance with response protocols is not the only thing that comes into play. Other obligations apply relating to breach notification, privacy regulations, privilege, contracts, and more. It is crucial to have processes in place to maintain compliance and mitigate an incident. Everyone needs to receive training and direction on any cyber controls and electronic preferences the organization has decided fit within their comfort level. Risk management gaps generally stem from lack of communication – whether it be the absence of a comprehensive global framework or unbroken silos.

To mitigate risk and ensure everyone is operating within the appropriate risk parameters, look for tools and systems that work across the organization as opposed to one specific unit. This can include software that can automatically detects compliance violations, automated information governance tools, secure data sharing applications, and more. Legal and other key actors should have a seat at the table for discussions with the cyber team to discuss how cyber threats match up with risk tolerance and which tools can create a compliant work environment. This should happen yearly, at minimum, to maintain an effective risk management program.

To learn more about this topic, please listen to our cyberside chats podcast.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Breaking Data Development: New Privacy Protections for US-EU Transfers Coming

Yet another international data transfer update recently materialized. On October 7, President Biden signed an executive order directing the steps to implement a new data privacy framework. This would apply to the flow of personal information between the U.S. and EU. This has been a long time coming since the Schrems II court decision in 2020 which invalidated the Privacy Shield framework as a mechanism to effectuate cross-border data transfers. The prior framework was in place for many years and offered a streamlined way to transfer U.S. to EU data. It was invalidated after Schrems II due to concerns over diminished privacy protections in violation of the General Data Protection Regulation (GDPR) and apprehension over U.S. surveillance during transfer activities.

Since the U.S. and Europe frequently conduct cross-border business activities in many different markets, the absence of a streamlined transfer process has presented major issues requiring expedient remediation. The EU does not recognize the U.S. as having data privacy laws or safeguards that would be adequate under the GDPR, so the only way to transfer information over the last two years has been via the EU's updated standard contractual clauses (SCCs). This is a more complex and unpredictable way to effectuate transfers and requires data transfer impact assessments that are time-consuming. As such, organizations have been anxiously waiting for the new framework to be finalized since there was chatter that it was in the works earlier this year.

The Executive Order

The new framework, which is being referred to as the "Privacy Shield 2.0," aims to address the EU's ongoing privacy concerns and will once again offer a more streamlined way to effectuate U.S. to EU data transfers. Here are the key points noted in the executive order:

- Robust review process: There will be multi-layer review available for EU residents to turn to if they have non-compliance issues. First, the Office of the Director of National Intelligence will investigate claims and have authority to issue binding orders. Such decisions will be subject to review by an independent data protection review court. This court will be composed of judges outside the U.S. government who will have full authority to adjudicate matters and order remedies to redress any harm suffered. A special advocate will also be available to the complainant during the court proceedings.

- Enhanced intelligence safeguards: U.S. intelligence agencies will only be able to access data in limited defined situations when needed to protect national security, specifically in instances involving validated intelligence priorities. The agencies must consider privacy and civil liberties for everyone, regardless of nationality or residential country.

- Mandated updates: All U.S. intelligence organizations must revise current policies and procedures so they align with the enhanced protections under the framework. The Privacy and Civil Liberties Oversight Board will review such revisions and provide annual reviews over any redress orders issued.

Overall, the executive order affirmed that the framework will greatly increase oversight and review of data transfers. Organizations are also expected to be able to self-certify compliance under the framework via the U.S. Department of Commerce when processing incoming EU data.

Next Steps

The EU now needs to review such framework and affirm whether it offers adequate protection in line with the GDPR's provisions. Analysts are split on whether this framework will truly address the privacy gaps between these countries, with some believing the protections are adequate and will pave the way for a U.S. federal privacy bill to finally materialize. Others doubt the framework's sufficiency and feel it does not sufficiently address commercial use of personal data, which has been a major debate over the past few years.

Regardless of outcome, the EU's decision to issue an adequacy decision or reject the framework is expected to take months, so lack of clarity on how to handle transfers remains until that time. For now, affected organizations need to continue to play the waiting game and rely on SCCs for data transfers. However, while many organizations dropped their privacy shield certifications after the Schrems II decision, there are still a good amount that are maintaining them even though not in use. Some analysts are advising these organizations to keep up their certifications as it would make for an easier transition when and if the new framework becomes effective. Now is the time for leadership, legal, and privacy teams to be strategic about this decision. A good formula to use is balancing the cost of certification maintenance with the benefit of expediting transfer backlog and overall risk.

For more insight on data transfers, please read International Data Transfers: Knowing Which Rules Apply to Comply.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

CLM 101: Understanding the Basics and Benefits

Contract management has been giving the legal industry headaches for years. Many legal teams struggle with managing or analyzing contracts effectively – partly because of the volume to sort through but also because of the lack of proper processes in place backed by the right technology. While going through contracts will lead to better classification habits, this can also help teams pinpoint inefficient or litigious clauses, draft better templates, determine if obligations can be prepaid at lower rates, reduce storage needs, remain compliant under new regulations, and quantify many types of organizational risk. Enter contract lifecycle management (CLM), an underutilized tool on the market for years. By understanding the value of CLM tools, legal teams can start to better manage their contracts and learn how to tell a story with data derived from their contracts. This is turn assists with the greater initiative of demonstrating legal's value to the entire enterprise.

What is CLM?

Contract deadlines and obligations vary depending on several factors. This includes the nature of the agreement, client preferences, regulatory oversight, and more. Lifecycle management, review, and obligation tracking can be overwhelming – especially when dealing with a high volume of commercial contracts. CLM tools provide a way to optimize the creation, execution, storage, and ongoing management of contracts. This technology can apply from the request phase through negotiations to reporting. It can also be used to collect and coherently organize and code already existing contracts. Implementing CLM workflows and technology into practice allows legal teams to be more thoughtful and proactive with managing the entire tenure of their contracts.

More teams are starting to turn to consulting firms to evaluate, implement, and integrate tools into operations. New CLM solutions on the market offer more advanced capabilities powered by AI allowing for data extraction, clause suggestions during authoring, obligation management, and risk analysis.

Adoption Rate and Benefits

With the overwhelming need to use a consistent standard for storing and managing legal documentation, it is surprising that CLM tools have not yet gained widespread adoption. While investment and use has definitely grown over the past few years, there are still adoption gaps – especially when it comes to understanding expanded value opportunities. This can likely be attributed to not knowing where to start, lack of understanding potential ROI, and overall absence of education on advanced capabilities or data insights these solutions can offer. Coupling CLM tools with expert review helps legal teams achieve a robust contract management program. Exploring these partnerships is one way for organizations to lessen the fear surrounding CLM integration and enhance widespread education on this topic.

Here are five key benefits that CLM tools can offer legal teams:

- **Organization:** The most obvious benefit is the ability to have an adaptable database of record with improved access to up-to-date and properly attributed contracts. Having such a system in place eliminates contract backlogs, makes it much easier to retrieve agreements, and reduces storage.

- **Speed:** In addition to streamlining contract retrieval, CLM tools speed up new contract drafting and ongoing management. This is due to the ability to automate simple drafting tasks and the advanced AI tech that can quickly illuminate important issues during negotiation or risk analysis. Automation also gives the legal team time back to focus on higher level contracting tasks such as negotiation and regulatory reporting.
- **Consistency:** Having better organized contracts helps determine where automation and standardized agreements can apply, which in turn makes drafting new contracts and obligation tracking much simpler. This also improves defensibility.
- **Agility:** When using CLM tools to draft templates or create model clauses, it is easier for teams to pivot when departures are needed. For example, if a standard clause proves to be litigious it will be easier to pinpoint the problem and make quick changes to the template. Additionally, when a new regulation comes into force teams can react faster and determine which agreements are affected and what needs to be amended going forward to remain compliant.
- **Risk:** Some CLM tools can analyze past agreements and rank risk when negotiating a new deal. This is extremely beneficial to the client and helps teams quantify various types of organizational risk that exist.

All of the above benefits feed into better and more efficient work product at lower costs. As with most new legal tools, the upfront costs can seem steep but having a repeatable trusted process leads to unmatched ROI that leadership can get behind with the right metrics to illustrate cost effectiveness.

Conclusion

With more contracting tools, consulting firms, and legal operations professionals entering the market and advocating for CLM, legal teams will begin to have a more sophisticated understanding of this technology. Fair predictions in this space include more partnerships with consulting firms that can advise and help with implementation; smaller initial investments that allow for use case testing before creating more robust CLM programs; greater focus on security as threat actors continue to explore new ways to carry out attacks; and the elevated need to have candid discussions with leadership about where CLM fits into the legal tech budget and whether current budgets are realistic. While this all may affect adoption rates in the short-term, increasing tech education will help legal teams understand potential value drivers and use cases available.

To learn more about how Epiq can help you, click here.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Cryptocurrency and Bankruptcy – The Unknown Frontier

Currencies have evolved since the introduction of global blockchain technology twenty years ago. Blockchain is a complex technology that powers the creation of cryptocurrencies like Bitcoin and facilitates other digital distributed ledger transactions. With more people investing in crypto assets now more than ever before, the global digital currency market is likely to grow over the next decade. However, the future remains unknown as this year's crypto market crash lead to the first bankruptcy filings by cryptocurrency lending platforms. It is crucial to monitor how the bankruptcy courts treat digital assets and creditors as this will have a hand in future market trends.

The History of Currency

After World War II, the Bretton Woods pact became effective making the U.S. dollar the dominant global currency backed by gold reserves. In 1971, President Nixon decoupled the dollar from the gold standard, however, the dollar has remained the dominant form of global currency. Today, the fiat currency model still prevails as a benchmark for global transaction values. The regulated currency and banking systems in the U.S. operate within a centralized finance structure backed by multiple layers of monitoring and compliance. For example, investors around the world have trust in the U.S. dollar because it is secured by the full faith and credit of the government, subject to reporting by multiple agencies, and the deposits are FDIC insured. These protections provide an inherent sense of security and make it easier to transact with other countries that also use fiat currency.

In 2009, cryptocurrency was introduced as a new asset which was supported by blockchain technology. There is now a wide array of digital currencies available for investment. These decentralized finance options are in the form of tokens or coins which are algorithm-created, uninsured, and not regulated by any agency of the federal or state governments. With decentralized finance exchanges investors are, in some instances, surrendering their crypto assets to an unregulated entity which in turn may leverage that asset without proper consumer protections. The absence of any governmental oversight with the associated fees of intermediaries has proved very appealing to many investors. The popularity of crypto

investing has grown over the past 14 years. Even so, the total market share of the crypto asset sector today totals around $1.5 trillion. The current crypto market crash aka "the 2022 crypto winter" has resulted in an increase in bankruptcy filings. How these matters play out will continue to shed light on the sector as a viable asset class for future investments.

Recent Bankruptcies

In July 2022, cryptocurrency trading platforms Voyager Digital and Celsius Networks filed for chapter 11 bankruptcy. Customers can no longer withdraw, swap, or transfer crypto assets from their accounts during the pending reorganizations. While representatives from Voyager have indicated that deposits made with U.S. dollars are expected to be credited back to customers, this is a legal issue pending before the court who will decide the ultimate ownership disposition of the currency held in the bankruptcy estate. In September, a large crypto-mining data center Compute North also filed for chapter 11 bankruptcy. It will prove interesting to observe how the court treats the reorganization plans presented by each company. Others have chosen to liquidate, including crypto hedge fund company Three Arrows Capital. The hedge fund could not secure a viable plan to reorganize its operations and turned to an orderly liquidation.

Several unique issues surround this type of bankruptcy action, including the following:

- Due to the lack of transparency and clarity about the status of the ownership of the crypto currency on deposit, many crypto investors were under the impression that their transactions were insured or protected in some manner and that they retained full ownership rights. As noted, ownership rights will vary depending on the terms of the underlying customer contract.
- Current disputes are also ongoing about whether a decentralized finance loan should be considered a registered security instead of a currency. Several private lawsuits addressing this question are currently pending in several states.

It will be interesting to observe how these, and other key factors, play out in bankruptcy courts and reorganization plans.

Predictions

The intersection of cryptocurrency and bankruptcy presents a unique opportunity for the courts to have a hand in shaping the future security of these new assets. The decisions made by the bankruptcy courts could expediate the regulatory framework required to support a robust crypto currency market, but this will evolve over time as these cases go through the chapter 11 process. Here are five predictions on what could materialize in the cryptocurrency sector:

- While the popularity of cryptocurrency as an asset class is expected to grow, many potential investors are watching these chapter 11 cases intently to ascertain how these assets will be treated when faced with financial challenges. Whether increased scrutiny and regulation will emerge will depend on the ownership rights allocated by the court and the associated rate of recovery on those claims.
- More crypto lending platforms and other companies operating in this market will file for bankruptcy if valuations do not stabilize in the coming months. This will present more opportunities for the courts to have a hand in defining the bankruptcy parameters around the future of cryptocurrency.
- There will be increased pressure to decide whether certain crypto coins should be classified as a security or currency. If courts decide that a digital currency should be classified as a security, lending platforms will need to register with an exchange and those assets will be regulated by an agency of the U.S. government.
- Other cryptocurrency companies will consider buying distressed lending platforms in an effort to rescue the crypto assets. Both Voyager and Celsius have already received and denied acquisition proposals, but other companies continue to attempt buyouts of these platforms so this could be a crucial part of their reorganization plans.

Conclusion

It is unknown whether a decentralized finance model will ever prevail as dominant currency, but as of now it is safe to say that this is not a possibility. With crypto prices dropping and bankruptcies surfacing, usage will likely stall until more clarity is provided on the ambiguities discussed above. Customers of struggling lending platforms are playing the waiting game until restructuring plans and favorable decisions unfold in the bankruptcy courts. It will be interesting to see what is in store for the future of crypto and what role these bankruptcies will play in the larger global economy.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Retaining In-House Talent Through Transformation

The talent war remains strong in the legal industry as many lawyers are making career choices through a different lens. Over the past few years, there has been a shift to prioritizing work-life balance and an organization's value-driven initiatives when determining whether to stay or seek different opportunities. Historically, much of the legal industry has been driven by pay so this change has called for general counsel to factor retention into their legal transformation strategies. This requires making it a strategic priority with defined goals, specific values, and tangible tactics. While trending retention efforts focus on providing flexible working arrangements, reducing diversity, equity, and inclusion (DEI) gaps, and prioritizing mental health in the workplace – ensuring the right work is being done by the right hands is another large piece of the puzzle.

Most legal teams have explored outsourcing opportunities to some degree over the last decade to help with overflows of administrative work. However, the ability to truly add value and keep the legal team happy goes beyond reducing the administrative burden.

Here are three components that general counsel should consider adding to their retention strategy:

- **Balanced Automation:** Outfit the legal team with technology that will help their specific practice, which will vary. Instilling automation wherever possible helps with this feat, but it is important to not burden staff with too many tools and find the right balance. Automating the right workflows will limit time spent on repetitive tasks and promote uniformity. Options to explore include eSignature tools, templates, legal invoice review software, and matter management solutions. Selecting and implementing new systems requires significant effort and time, so it is important to focus on what the team needs to work remotely effectively.

- **Rethinking Thoughtful Legal Workflow Design:** With much of the legal workforce seeking better-balanced jobs, it is crucial to have the legal team do legal work. This alone holds retentive value. Lawyers feel more valued when they are utilizing their expertise, focusing more on strategic tasks, and have ample support. To achieve this, ensure the legal team has enough resources in place to be able to focus on their highest value work for the organization. This also lends itself towards improved promotion and internal career pathing. Rethink end-to-end workflow, implement tools to reduce the burden of larger quasi-legal matters such as contract management, leverage non-legal resources where appropriate, and regularly evaluate opportunities to "junior-ize" work.

- **Extend Partners, Including Alternative Legal Service Providers (ALSPs):** Oftentimes when a full-time employee quits, the organization does not have immediate resources available internally to fill the role. A way to bridge this gap is to evaluate where models such as legal talent secondments can relieve overflow pressure following attrition. This is also an efficient and cost-effective way to maintain continuity during the long-term permanent hire process or when a specific project calls for specialized expertise. The legal team will not get burned out by extra work while management is recruiting to fill a vacant role or if a large matter requires extra resources not feasible internally.

Another way to utilize outside partners effectively is for repetitive, high volume, non-commercial legal work. General counsel should identify where joint-delivery models could be beneficial, such as managed contract review to answer client questions across material contract volumes.

Conclusion

With many legal departments facing regrettable attrition amidst the resignation wave, current market volatility, and continued impacts from the pandemic – retention of in-house legal talent is a business continuity imperative. While competitive pay will always be a driving factor, it is no longer enough alone to support retention efforts. More lawyers now want to see their organizations investing in optimal technology and partnerships to balance the team's workload and highlight specific skillsets. This allows for more professional growth opportunities while maintaining high quality work product. This, coupled with value-driven initiatives such as advancing DEI and prioritizing mental health will foster a better-balanced and fulfilling working environment.

If you enjoyed this blog, consider listening to our webcast on the same topic.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Mass Tort Transformation Opportunities: Where to Begin?

The legal industry has been undergoing major changes over recent years. Both corporations and law firms are paying more attention to the macrotrends surfacing across the industry and taking action to align with competitors and meet evolving client needs. These trends include tremendous cost pressure, modern technology, increased regulation and compliance, more cyber-attacks, and a shift to outcomes. The underlying theme? Legal is a business that is transforming to keep up with opportunities and challenges present in the digital world. Legal teams are searching for ways to accomplish the most with the least while still maintaining efficiencies and improving outcomes. While this may seem like a tall order, it is more easily accomplished with the right provider partner.

Mass tort is an area where transformation opportunities abound. Leveraging the right technology in this space can deliver optimal results and finetune processes so repeat matters run even smoother.

Challenges

Doing more with less requires the right mix of not only people, process, and technology – but also data. With mass tort, using the best tools will put the most money in the pockets of those affected in the most efficient manner. From product liability to personal injury, large-scale catastrophes or malfunctioning medical devices, mass tort cases derive from a variety of incidents and actions — some intentional, others accidental. What they all share in common is the fact that there were injuries suffered, frequently in large numbers. Settlement is often the preferred resolution path, as the goal for all parties involved is to remedy the harm and move forward. However, it can be difficult for firms to manage these cases as there are so many moving parts and looming deadlines.

Here are common challenges that arise with mass tort administration:

- **Communication:** Just like class actions, mass tort cases have many plaintiffs. It can be challenging for mass tort firms and defense counsel to efficiently effectuate widespread communication about case updates or settlement administration. However, the level of difficulty does not change the ethical obligation owed by all attorneys involved. From telephone calls to letters, email, and texts – using a back-office approach presents opportunity to appropriately scale outreach to keep clients informed.

- **Cost:** The cost of maintaining a staff to perform the work required for a mass tort case coupled with the actual costs of working up the case can be daunting. However, the right technology can target inefficiencies. This in turn makes costs more affordable, permits attorneys and their staff to focus on the legal aspects of the case, and yields better results.

- **Case development:** Each mass tort case has to be worked up and proven, similar to that of a stand-alone personal injury case. It can therefore be difficult for mass tort firms and in-house defense counsel to gather documentation from each plaintiff, analyze medical records, and go through the discovery process, whether in a MultiDistrict litigation setting or not.

These burdens can be impossible to carry alone when it comes to large mass tort matters. Teams can remove such challenges by working with a provider partner that scales talent, uses proven processes, incorporates optimal technologies, and taps into data driven insights. Many legal organizations are riding the technology treadmill looking for solutions that are faster, less costly, and better than others on the market. This seems

like an impossible feat, but it becomes feasible when working with a provider that possesses such qualities.

Getting off the Treadmill

Transformation can come in many forms, but generally happens when legal teams strategize and make case decisions through a business lens. Jumping off the legal tech treadmill is possible with a partner whose core processes are complimented by the people they employ and who know how to effectively leverage technology to deliver results.

Here are key qualities that mass tort litigators should search for in such a partnership:

- **They are faster because of experience not expediency.** Attractive offerings to explore include data integration capabilities, ability to reduce lien resolution timelines through data exchanges, and automated electronic claims payments, depending on payee.
- **They are more cost-effective because of the ability to streamline process.** Data integration reduces manual input. Providers that can serve as a back office and utilize machine learning tools, when necessary, will also advance cost reduction strategies.
- **They are better because of the simple fact that leveraged experience assures outcomes.** Lastly, look for a partner that can clearly illustrate results and regularly provide updates. Examples include lien reduction history, real-time dashboard offerings, analytics that help teams make smarter decisions, and smarter medical record review to unearth key insights to inform settlement talks between all parties involved.

Above all, when selecting a provider partner remember that technology should be the catalyst. Technology-enabled solutions inform the right bets and help teams get off the treadmill. Experience is needed to know which best-in-class technologies will deliver money to harmed individuals faster – which is beneficial to both plaintiff firms and defense counsel. Mass tort is a complicated area of law where legal, medical, and administrative often converge. To turn the complex into something more simple, attorneys should look for the opportunity to transform mass tort administration through more strategic decisions and cooperation between parties that are enabled by partners offering optimal tools and resources to expedite the process to finish what the attorneys started.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

The Emerging Role of the Lawyer/ Technologist in Antitrust Matters

The increasing sophistication of analytics tools available to lawyers coupled with the skills of the outsourced team containing technologists and lawyers raises the question of whether focusing on the review of "documents" still makes sense. In the days of paper discovery, a document was a finite compilation of information that had no necessary relationship to other documents unless legal counsel developed that larger context. Today, technology provides tools and processes that can assess the document in context (e.g., by compiling an entire email "thread"), find documents that are similar, and provide detailed information about the pattern of communication surrounding the document. These capabilities provide a greater lens for exploring documents in a contextualized setting.

Complexities in electronic communications are further compounded and complicated by applications used for workplace collaboration and shared documents. Edits do not occur on a single paper version anymore. By focusing on the data more broadly, lawyers can think about the information it contains and how it affects their view of the matter. This applies across the board to litigated cases, merger reviews in front of an antitrust regulator, and internal corporate investigations. By working closely with the technology team, lawyers can develop intelligence early in a case that provides a strategic advantage, such has whether to settle the case or make an application for leniency in a potentially criminal setting.

The Shift from Documents to Data

It may be semantics, but the question should now be asked whether the exercise of discovery is really the analysis and assessment of data rather than the methodical review of documents. The focus on data can alleviate slavish adherence to a review methodology that is premised on an entirely different set of circumstances. The focus on documents creates a perspective that is limited in scope. By looking at data, the legal team can quickly develop a hierarchy of key facts and themes to help stratify review and analysis. The legal team can also deploy rigorous testing processes to validate the results of the Technology Assisted Review (TAR) process.

Benefits of Early Assessment

Taking some extra time on the front end of a new matter will undoubtedly save time and money, but can also inform case strategy throughout discovery and up through trial. By analyzing a data set during the early case assessment (ECA) phase, counsel can unveil pitfalls that may not become evident until much further down the road. This can be devastating with large-scale matters that must adhere to a tight production timeline. Understanding the data characteristics of a given population ensures adequate time to remediate any data issues prior to production. It also affords an opportunity to assess the potential risk regarding pending legal issues, as well as unknown and potentially damaging issues. In many instances a thorough investigation will reveal key documents that afford the legal team an opportunity to perform tactical fact development and build their case before, or in tandem with, document review. Early analysis can also identify challenges that may slow or impede a review such as high volumes of privileged content, documents needing redactions, and privacy concerns.

Each new data set and case introduces unique elements that need to be examined in the context of the specific end goal. Understanding data from a technical perspective is key, but arguably not the sole consideration. In an environment where antitrust enforcement actions and merger challenges are increasing while pressure is also mounting to keep costs low and maximize efficiency, it is imperative to perform a

preliminary factual analysis before executing a document review. Make it a priority to understand the anticipated responsiveness level within the dataset, prevalent issues, and potentially damaging documents. Additionally, early insight regarding the estimated effort for a privilege review and log can set the stage for better-informed strategy. This will foster a successful and well-managed document review.

Implementing the Process

The analysis should be performed by someone who is highly competent. In many cases this is someone with a legal background and subject matter expertise in the matter who can spot issues and quickly identify the most useful or inflammatory content. Ideally this individual also will be proficient in legal technology, an expert in data interrogation, and possess the capabilities to perform the requisite analysis. Enter the lawyer/legal technologist.

There has been an increase in these types of roles at law firms and corporations. These professionals are becoming essential to modern day eDiscovery. For those that do not have a lawyer with these qualifications on staff, it becomes increasingly important to partner with a trusted service provider that can offer guidance and execute the analysis under the direction of the legal team.

This blog post is derived from the Chapter titled "Outsourced Document Review: Data Intelligence, Technologist Lawyers, Advocacy Support" by Edward Burke and Allison Dunham, which appears in the Thomson Reuters treatise eDiscovery for Corporate Counsel (2022). Reprinted with permission, © 2022, Thomson Reuters. Jason Butler also contributed to this blog.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Lawyers and Cooperation: The Ongoing Hurdle

How can two adversaries learn to cooperate? That has been the burning question amongst litigators over the past seven years. On Dec. 1, 2015, significant amendments to the Federal Rules of Civil Procedure (FRCP) became effective. While the word "cooperation" was not expressly included in the amended rules, it was understood through the notes and drafting discussions that the changes encourage parties to work together earlier and more often to reach a resolution. This seemed like an impossible feat. The thought of cooperative adversaries is quite the oxymoron. Surprisingly, some strides have been made – but there is still a long road ahead.

Now that seven years have passed, it is an opportune time to analyze where litigators stand today with cooperation. Has anything changed? Will the rules need further clarification to truly push cooperative strategies? How have the courts weighed in on this topic? How is technology playing a role in cooperation? Read on to delve deeper into these questions and for predictions on what is to unfold by the ten-year anniversary of these amendments.

Looking Back: A Recap of the Rule Changes

The 2015 amendments encourage discovery proportionality, party cooperation, and earlier court engagement. Some key changes included parties sharing responsibility with the court to reach just resolutions quickly and inexpensively, emphasizing proportionality at every step of the discovery process, stipulation on discovery sequencing, and the ability to send production requests before a Rule 26(f) conference. The goal was to better control costs and reach outcomes more efficiently. With litigation being adversarial in nature, there was immediate confusion on how two adversaries can cooperate. Putting these terms together does not seem to mesh, but adversarial cooperation has been the standard that the judicial system is striving to reach.

Although the amendments were meant to foster party cooperation, this was not expressly included in the rules, making it unclear how far a party needs to go to be deemed cooperative. Some guidance came in the form of a note to FRCP 1, which required the just, speedy, and inexpensive determination of every action. The note stated that parties share responsibility to employ the rules and most cooperate

to achieve those ends. Additionally, it is key to stray away from over-use, misuse, and abuse of procedural tools that can be costly and delay the case.

The Current State of Cooperation

With little guidance on where strategy and cooperation merge, many in the legal community predicted that ambiguity would remain as to how much cooperation is required. Initial questions surfaced around when parties need to cooperate, necessary technology disclosures, availability of sanctions, and more. Almost a decade later, where do things stand? As with most legal issues, the answer is unclear. After so many years, the legal community as a whole appears to be working towards more cooperative practices but is still plagued with defining a standard to drive such cooperation. Here are three key observations to note:

- Recurring case law themes each year have centered around defining proportionality, aligning sanctions with the realities of emerging technology, and leaving eDiscovery protocols and technology usage up to the parties. Since the pandemic, more courts have also ordered parties to work together to solve discovery issues and avoid motions wherever possible. A surfacing trend appears to be judges issuing sanctions for delaying matters by failing to solve discovery issues efficiently without court intervention. This comes as no surprise as many judges are trying to tackle heavy backlogs. Cooperation definitely

plays a role in all of these scenarios.

- The pandemic forced party cooperation which could help pave the way for future clarity and best practices. Lawyers essentially had no choice but to embrace collaborative tools and work together to make remote proceedings successful. The 2022 supplement to the Sedona Conference Cooperation Proclamation noted: "Successful remote and hybrid proceedings require an even greater degree of cooperation between the parties than is strictly required by the rules. No longer can opposing counsel appear at a deposition and blithely agree to the 'usual stipulations,' whatever those might be. In the remote or hybrid environment, all pretrial proceedings require advance planning and agreement on the platform to be used, the persons to be involved, the handling of evidence, etc."
- The rules will need to undergo further amendments to create an actual duty to cooperate. It is true that the needle has moved and more lawyers seem at least willing to collaborate and continue to find value in working together. More courts are endorsing the Sedona Conference Cooperation Proclamation and are encouraging parties to handle discovery conflicts out of court. However, without an affirmative duty to cooperate the issue will continue to remain ambiguous and merely be weaved into court decisions without clear definition of what cooperation entails under the rules.

So, what does this all mean? From a case law perspective, cooperation is an element of recurring themes even if not specifically stated. The courts will likely continue to order parties to resolve issues amongst one another and agree to technology protocols. It will be interesting to see how sanctions continue to unfold in this regard. However, it is unlikely that a court will affirmatively create a "cooperation standard" until it is expressly embedded in the rules. Will this happen before the ten-year anniversary of the 2015 amendments? Or will it ever happen? This remains uncertain. On the one hand, lawmakers had major reservations about the backlash that could result which is definitely still a concern. On the other hand, more parties are willing to cooperate, technology is fostering better collaboration, and courts are getting increasingly fed up with counsel advancing discovery tactics that cause unnecessary delays. One thing that is for certain is that if further amendments occur, the courts will play a major role in defining the cooperation standard – so stay tuned.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Ten Use Cases for Portable AI Models

In recent years there has been a noticeable shift in the legal community from hesitation around using emerging technologies to embracing modern tools that can optimize process and improve cost management. Legal teams that were once set in their ways and skeptical of technology now are looking for automated tools that can improve efficiency at every level. Portable AI models are the new tool on the scene that can help with not only eDiscovery review, but so much more. These tools reuse prior insights to jumpstart review, eliminating the need to create and train a new model every time a similar matter or question arises.

The first type available is a pre-built model that can help identify language in datasets on repeat topics such as privileged content or insulting behavior. The second type is a customized bespoke model trained to pinpoint issues or answer questions unique to a particular organization. Generally, a service provider will have a library of pre-built models on common topics for clients to easily utilize. Custom models will require working with a service provider to internally train unique models. Both types of portable AI models have continuous evolution potential and can be a key value generator for legal teams.

Use Cases

The use cases for portable AI models are growing, the technology is more powerful than ever, and application can reach outside the legal department. Current awareness around how many use cases are out there is lacking, but this will absolutely change as adoption grows. This can only happen with more education opportunities on application and ROI potential.

Here are ten use cases where AI models can prove useful in litigation, investigations, and beyond:

Culling data for document review

1. **Privilege review:** During the eDiscovery process, the privilege review phase can be cumbersome. Applying a pre-built model from a provider that is trained to target privilege language can be a huge aid in

privilege identification and the redaction process. This will streamline eDiscovery review while maintaining confidentiality where appropriate.

2. **Sensitive data identification**: A model targeting certain words or phrases that indicate misconduct has proven especially effective in employment litigation. For example, in a sexual harassment case teams can apply AI models on communication data to pinpoint sexually explicit themes, concepts, and language. This software can also detect comments on appearance, bullying, discrimination, harassment, and/or threatening behavior. This can help parties jumpstart review by identifying key actors and witnesses earlier.

3. **Litigation risk analysis:** Teams can apply portable models before even reach the eDiscovery phase as another way to perform early case assessment and make decisions about settlement. Using the employment situation discussed above, having the ability to run a pre-built sensitive language model during the investigatory phase could save an organization the expense of moving forward with a case if it is more suited for settlement or dismissal.

4. **Pinpointing valuable keywords:** This is an illustration of how layering tech can yield more efficient results. The legal team can first use a pre-built model to determine optimal keywords. Then, they can use the keywords in conjunction with other tools to further cull the dataset and pull out what is necessary for manual review.

5. **Custodian identification:** A challenging and time-consuming part of eDiscovery can be identifying where pertinent data resides. Although there is other tech as well as information governance strategies that can help with this feat, using a portable AI model is just another beneficial tool to explore. This application is especially helpful where organizations have built bespoke models that have already been customized to account for unique internal workflows and data repositories.

Regulatory compliance functions

6. **Data elimination:** Just as with litigation, both pre-built and custom AI models will be useful during a regulatory investigation to cull cumbersome datasets. Many regulatory bodies impose stricter deadlines, making tools that can expedite review necessary to remain compliant. This is also an effective way to cut costs, as investigative budgets are generally smaller.

7. **Internal investigations:** Teams can deploy models that will assign a sentiment score to prioritize evidence hotspots or detect fraudulent behavior that would raise compliance risk. For example, a model geared towards kickbacks, insider trading, or related topics can help detect fraudulent patterns that are the subject of an internal investigation. By running a pre-built model on the data, teams can uncover which custodians are using words and phrases indicating the fraudulent behavior so they can quickly act.

8. **DSAR compliance:** Under the GDPR, consumers can request access to see how organizations are using their data. Since quick turnaround is required, an AI model already trained to identify personal information sources (which can come in many forms) can help teams achieve compliance fully and expediently.

9. **Monitoring internal behavior:** This application is beneficial in the financial services industry. Leadership can use a model to monitor employee behavior to ensure that employees are acting appropriately and not promising their clients unattainable rates or assets.

Data breach response

10. **Post-breach analysis:** Applying an AI model after a breach occurs can help narrow down who to notify and where sensitive data resides. Time is of the essence in these situations, so being able to quickly apply a tool like this will greatly aid in mitigation efforts.

Conclusion

Portable AI models are the new tech tools to watch. The use cases and maturity will only continue to expand as more organizations become aware of how these models work and what benefits they can offer to legal and other departments. This is a tool that not only saves on cost and time, but also promotes efficiency and consistency. Now is the time to monitor new industry and court developments, evaluate investment opportunities with providers offering pre-built or bespoke models, and discuss potential use cases with leadership teams.

To learn more about portable AI models, consider reading our recent whitepaper on the topic.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Managing International Legal Holds in the Era of Data Protection: Eight Practice Points

Implementing legal holds quickly and effectively is key to maintaining defensibility during litigation and investigations. When a matter involves U.S. law, parties have a duty to preserve relevant information once litigation is reasonably anticipated. To maintain compliance, altering retention policies and sending legal hold notices to all potential custodians are crucial steps for avoiding future spoliation sanctions. To help parties understand their preservation duties, in 2010 and 2019 the Sedona Conference published commentaries providing guidance on legal holds covering triggers and process.

In the updated 2019 version, a new guideline directed organizations to be mindful of local data protection laws and regulations when initiating a legal hold and planning legal hold policy outside of U.S. borders. This prompted Sedona to create an international-focused commentary to help legal teams understand and navigate the complexities cross-border matters can bring, which is amplified by the current privacy landscape. Public comment closed at the end of this October on "The Sedona Conference Commentary on Managing International Legal Holds," so it is important to monitor when the final version is published. It is unlikely that any changes would be significant, so now is the time for legal teams to start considering the practice points noted in the commentary.

Data Privacy Challenges

Implementing legal hold plans can decrease the risk associated with inadvertent spoliation and increase the chances of successful outcomes. A well-developed plan allows legal teams to better manage matter costs while decreasing the chances of lost data, time, or strategy advantages. With the rise in data and international transactions, more cases and investigations are involving parties and data located outside of U.S. borders. International legal holds, which arise when preservation obligations cross international borders, can present unique obstacles leading to matter delays and increased expenditures. The biggest challenge is when preservation conflicts with restrictive international data protection laws.

For example, the General Data Protection Regulation (GDPR) contains binding principles applying to data preservation. The law directs data controllers to conduct processing activities

involving personal information with lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability. GDPR articles five and six contain more detail on these obligations. If counsel does not consider such requirements during a case or investigation involving both the U.S. and an EU member state, then penalties may result for unlawful processing activities. Several other nations have also followed suit and implemented similar protections and requirements in their data privacy regulations.

Sedona Recommendations

The commentary mainly focuses on how U.S. preservation duties interact with GDPR requirements. Since the majority of updated international data protection laws are based on the GDPR to some degree, the framework is meant to apply in situations involving other nations as well. The commentary suggests that practitioners should review and consider the following eight practice points for managing international legal holds.

1. **Determine Whether the Preservation of Personal Data Is Necessary, and Then Determine Whether a Data Protection Law Applies:** In many instances, preservable information will contain personal identifiers. If the data controller is subject to the GDPR or other international regulation, then the team needs to perform a deeper analysis to remain compliant.

2. **Apply the Data Protection Law's Guiding Principles for Processing Personal Information to Every Preservation Step or Process:** Failure to take any binding data protection principles into account can result in penalties and cause delays. Counsel should implement extra protection measures mandated by international law to avoid negative outcomes. Also, do not forget to consider obligations relating to transfers of personal data across borders.

3. **Document the Lawful Basis for Preservation and Preservation Steps Taken Thereafter:** This is a requirement under the GDPR that will help maintain defensibility. Documentation should start as soon as a legal hold is triggered.

4. **Take Steps to Minimize the Scope of Preserved Information:** Data minimization is meant to promote consumer privacy interests by limiting processing and use to only what is absolutely necessary. This is manifesting as a focus in many new laws, so it is crucial to advance this principle when determining which data is subject to a legal hold. A best practice is diving deeper into the information a custodian has and limiting the legal hold language to relevant documents.

5. **Consider Involving Data Protection Officers, Supervisory Authorities, or Work Councils:** Keep in mind that this will be dependent on the specific circumstances and issues pertaining to a matter.

6. **Communicate Clearly with Data Subjects, Advising What Materials the Organization is Preserving, and What Steps Will be Taken as to Personal Information:** Communication and transparency are key to maintain compliance with both legal hold and data protection requirements. The GDPR mandates preservation notice to data subjects.

7. **Make Sure Legal Hold Notices are Translated in Accordance with Local Law:** When local law requires translation for business communications, it is best to interpret legal holds under this umbrella. Translation also aligns with the goal of being transparent during preservation and data processing activities.

8. **Reevaluate and Release Legal Holds and Dispose of Information When No Longer Needed:** If the scope changes, counsel should release information no longer needed. This promotes the principles of data minimization, purpose limitation, and storage limitation. It will also help teams focus on the most important information and better control costs.

Teams encountering international legal holds should consider integrating the above practice points in their legal hold programs. This is a good opportunity to partner with a consultant possessing deep experience in shaping, implementing, and managing data to ensure legal hold readiness. This will require the right strategies, expertise, and software. A partner that also has detailed knowledge and practice with data protection regulations such as the GDPR will be key to maintaining compliance, bringing clarity to the process, and offering confidence of reliable advanced planning.

If you enjoyed this blog, consider reading New Sedona Commentary Tells Us Protecting Privilege Can be Easy with Rule 502(d) Orders.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.

Cloud Adoption Accelerates in the Legal Industry: How Do ALSPs Factor Into Recent Trends?

Cloud technology continues to trend in the legal community as more organizations are taking a digital first approach and expanding remote capabilities. The first phase of cloud adoption has been in progress for years as a part of ongoing information governance efforts. Data migration has offered several benefits including removing the risk of physical destruction, flexible access, cost reduction related to storage, and easier information access.

Law firms and corporate legal departments are now accelerating cloud technology adoption not only for document management purposes, but also in other areas. Examples include talent management, marketing, and eDiscovery solutions. The 2022 LegalTech News Technology Survey 2022 saw an increase in law firms investing in cloud tech with 21 percent reporting a heavy increase and 64 percent a a slight increase in the tools they store in the cloud. It is crucial for organizations to track these trends and available benefits to determine which cloud model is the best fit. Specifically with eDiscovery, decisionmakers should delve deep into the value of using an alternative legal service provider (ALSP) to integrate a cloud platform versus direct purchase through the software vendor.

The Cloud and eDiscovery

In addition to the growing desire by legal teams to innovate, the cloud is trending in the eDiscovery space because many providers are decreasing or altogether removing on-prem solutions and moving to the cloud. Legal teams are responding by being more strategic with how they redefine eDiscovery investment, support, and process. The goal is to increase efficiencies by staying ahead of the curve with technology, which right now is focusing on operating in the cloud and the ability to back up data. The question then becomes whether to purchase cloud tech directly from a software vendor or have an ALSP assist with this transition.

The fundamental eDiscovery business model is based on service providers reselling software and hosting to support their investment in professional service capabilities that extend far beyond simply offering new tech. Expanded capabilities and expertise makes ALSPs the optimal choice for many when deciding to transition to a cloud-based eDiscovery model or to migrate data to the cloud for countless other business purposes.

Benefits of Utilizing an ALSP for eDiscovery Cloud Adoption

There is added value when accessing a cloud platform through an ALSP since they are built to provide professional services. It is true that purchasing directly allows access, initial implementation, and some training. However, that is essentially the end of the line as far as services are concerned. By accessing the platform via a properly sized ALSP instead, legal teams will still get these initial benefits and also the ability to derive so much more value from the investment. A quality ALSP will help legal teams understand how the platform fits into the broader ecosystem of eDiscovery products and services (including those provided by third parties) and how to create workflows that deploy it to best effect while remaining cost conscious.

Here are five major advantages of choosing an ALSP to access eDiscovery cloud technology:

- **End to end model:** ALSPs possess the capabilities to offer more than just the platform and implementation. They can also provide fully integrated ESI, information governance consulting, forensics capabilities, trial preparation assistance, and DRS programs. If there is need to leverage specific external resources on occasion, this will be easily accessible.
- **Expert knowledge:** Provider partnerships bring technology along with supplementary expertise about not just the cloud platform but also other specialized discovery processes and issues.
- **Flexibility:** In addition to the cloud technology, provider partners can craft a package of technology and services aligning with the legal team's specific requirements that is flexible enough to adapt to changing needs.
- **Ongoing software and workflow support:** ALSPs will liaise directly with the cloud platform provider to address any issues that arise. This can be time consuming and would fall on the legal team if purchasing directly. Additionally, if a particular matter requires a non-standard workflow or functionality not currently available on the platform, the team's provider partner will have alternative resources to reach a resolution.
- **Market insulation:** Accessing cloud services through a third-party provides an advantage in an ever-changing legal tech market. Organizations are able to choose best-of-breed technologies at every step to achieve optimal outcomes without compromising on features or performance. This can extend to alternative solutions to the main cloud platform when needed without the need to enter into separate contractual relationships.

Conclusion

Transformation requires understanding trending legal tech and determining the best way to incorporate it into current processes. This will look different for every organization. More cloud options will continue to emerge, so organizations need to continue monitoring trends and establish the best way to leverage cloud tech for eDiscovery and beyond. When deciding whether to buy direct or turn to an ALSP, it is crucial to account for the benefits listed above.

Visit blog post on the Epiq Angle

The contents of this article are intended to convey general information only and not to provide leagl advice opinions.