2023 Blog Book

epiq angle

epiq content

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.

Contents

epiq content

epiq content

New Year's Resolution for Lawyers: Learn More About Cyber Risk

Lawyers throughout the nation are gearing up to polish and execute their visions for the new year. Talks of strategy, budgets, goals, and professional development are circling the halls and video calls at legal departments and law firms. For those planning out continuing legal education (CLE) opportunities via online trainings, in-person seminars, and conferences – here is one piece of advice. Do not forget about cyber education. The practice of law and cybersecurity is more intertwined than ever before and must be a top priority for all lawyers.

The Intersection Between Cyber and Legal

Lawyers cannot effectively practice law today without some degree of knowledge about cybersecurity law, potential threats, and best practices. At the foundation of legal practice is confidentiality, competence, and candid communication. Cyber risk should be another foundational piece of legal education and training, as the two are very intertwined.

While the move to automated business processes and digital data management has been a key enabler for businesses, it comes with increased cybersecurity risks. These risks can threaten a lawyer's ability to act as effective counsel by inhibiting their ethical obligations. If a breach occurs, confidential data can be exposed publicly. Without knowledge of how technology operates and relevant security features, the ability to communicate over secure channels is compromised. This is why competence is key. In such a dynamic and dangerous cyber landscape education is necessary to remain competent and know how to manage cyber legal risk.

Cyber Education Best Practices

Remaining educated on cybersecurity risks and market trends will not only help lawyers protect sensitive client data, but also effectively advocate and advise for certain technology usage or strategy moves. For example, security issues will arise at every step of the discovery process – from determining where data resides and how it is stored to preservation, collection, and interception concerns. Having knowledge of the risks and solutions to solve issues at each stage will lessen the potential for case delays and breaches.

So, what type of cyber education should lawyers seek out to remain appropriately informed? While there is not one right answer to this question, a good first step is seeking out basic cyber knowledge. Stay up to date on trending attack methods. Understand the risks associated with the technology an organization is using or plans to obtain and take steps to change investments or add extra security measures to control threats. Some potential topics and courses to explore include cyber risks present in emerging technologies, incident response planning, information security laws, and cyber considerations during litigation.

The New York State Bar has officially recognized the importance of cyber education. New CLE requirements for lawyers take effect on July 1, 2023. They must obtain one hour of credit to satisfy their CLE requirement from the newly created Cybersecurity, Privacy and Data Protection category. This encompasses ethical obligations and general practice considerations that intertwine with these topics, providing a broad range of educational opportunities to explore. Credit earned earlier in the year 2023 will also apply.

Going Beyond the Bare Minimum

While more state bars will likely jump on the cyber-CLE bandwagon in time, lawyers in every state (and around the globe) should be incorporating cyber education into not only their CLE choices – but also everyday practices. The

requirement could increase over an hour in New York and any other jurisdictions that follow suit due to the expanding cyber landscape and increased threat potential.

Here are additional ways lawyers can boost cybersecurity knowledge beyond taking CLE credit:

- Subscribe to industry reports relating to trending attack methods and breach numbers.
- Get alerts on cybersecurity case law, such as class actions resulting from large breaches.
- Keep informed on bar opinions relating to cybersecurity, emerging technologies, remote working, and similar topics.
- Thoroughly vet all technology investments to understand any cyber risks and turn to provider partners for advice on optimal solutions that foster efficiency while safeguarding client data and proprietary information.
- Take advantage of internal cyber training and advocate for more when appropriate. Training offers benefits far beyond maintaining effectiveness as counsel and will be beneficial enterprise-wide. For example, oftentimes "cyber whistleblowers" that report problems to regulatory agencies or the public often do not have all the information relating to business risk decisions or complex technologies involved. The resulting investigatory response and reputation repair will utilize a lot of resources. This reality needs to be counterbalanced with valuable education that will promote transparency and expand cyber knowledge for everyone in the organization.
- Increase legal's involvement with incident response planning. Proactive planning prior to a cyber incident can save precious time after one occurs and ensure smooth service delivery when it counts most. While incident response heavily relies on technical and forensic actions, legal implications are just as important and will come into play at every phase of the response. Breach notification, impact assessment, privacy law compliance, and regulatory reporting are a few areas where the legal team will have an integral role in response efforts.

Cyber education has never been more important for the legal community than it is now. With more people working remotely and using a variety of emerging technologies, the risks of data compromise are amplified. Lawyers need to take extra steps to remain ethical, protect sensitive information, and properly advise clients. Make sure to add this as a resolution for the coming year!

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 Case Roundup: Protocols, Preservation, and Party Cooperation

As 2023 begins it is time once again to reflect on the most interesting eDiscovery cases from last year. Trends are always evolving in this dynamic space and eDiscovery professionals cannot afford to snooze on this review. What themes were practitioners seeing in the courts? How did that mirror or differ from the focus in years prior? Will these trends carry over into 2023? These are the questions to ponder at the beginning of each new year. Here is what came to light when reviewing key 2022 decisions:

- The effects from the pandemic are still present and courts are cracking down even further on delay tactics, failure to comply with court orders, and lack of party collaboration.
- More courts are issuing harsher sanctions. After the 2015 amendments to the Federal Rules of Civil Procedure, there was a trend of leniency and it was difficult to establish bad faith. Now judges are going back to issuing severe sanctions and making it known that cooperation, proportionality, and informed technology usage are key focuses.
- The remote working culture and increased reliance on technology continues to change the nature of litigation.
- Courts are starting to weigh in more on discovery protocols and specifically banning technology assisted review (TAR) usage in certain situations.

Five cases exemplifying these themes that are important to review before heading to court this year on cases involving similar issues.

Red Wolf Energy Trading, LLC v. BIA Capital Mgmt., LLC, No. 19-10119-MLW (D. Mass. Sept. 8, 2022)

The main issues in this labor and employment case were whether sanctions were warranted for counsel's delay tactics and how emerging technologies play a role in production. Plaintiff filed suit against a former employee for misappropriating trade secrets. Over the course of several years, plaintiff discovered missing documents

from defendants that were central to the case issues. Defendant kept producing key evidence that should have been discovered earlier on and after signing affidavits that production was complete. Defendant failed to work with plaintiff and adequately respond to discovery motions compelling production of key data, including Slack messages containing a "smoking gun" for Plaintiff's case arguments.

Plaintiff filed two sanctions motions which the court granted. Defendant attributed the faulty production to limited financial resources and the difficulty to extract Slack information, but this was refuted by expert testimony that a standard eDiscovery processing tool can handle Slack production at very low cost. This expert also discovered that it was likely some Slack channel data was deleted prior to production. The judge entered a default judgment noting that the law is not a game and this was very egregious discovery behavior.

This ruling illustrates the trend of judges entering harsh sanctions to reach justice. The judge made note that not only did these actions greatly prejudice Plaintiff, but also impeded the court's ability to manage the case and others on the overloaded docket. Courts are trying to play catch up from the pandemic and are no longer entertaining delay tactics, especially when they are repeated and avoidable. Another key takeaway is that ignorance on how to collect data from new tech sources will not be entertained. Litigators need to understand how collection works and there will likely be new standards in the future on what it acceptable for certain data types.

In re Allergan Biocell Textured Breast Implant Prods. Liab. Litig., MDL No. 2921 | Civil Action No. 2:19-md-2921 (BRM)(ESK) (D.N.J. Oct. 25, 2022)

This multidistrict litigation involved medical malpractice claims that textured breast implants and tissue expanders allegedly increased the risk of lymphoma for patients. A central discovery issue here was whether it is appropriate to deviate from (electronically stored information) ESI protocols. The short answer from this court? No. The parties previously agreed to search term and linear review. While review was in process, Defendants requested to modify the protocol and use TAR in conjunction with search terms. Plaintiffs objected to this change and the court agreed. Several reasons were given including the absence of cost analysis or sample testing to bolster Defendant's reasoning; that applying TAR after would only be reductive and not pull forward any new documents; and that the parties did not agree to this in the protocol or thereafter as a revision.

This case continues a theme that has repeated over the past few years: protocol language is extremely important and will govern how a judge decides discovery disputes. Some litigators may fear that this signals more court control over technology usage or never allow changes to protocols. However, if the protocol would have left the door open for TAR usage or the parties were able to cooperate and find a solution outside of court then the outcome would have likely been different. This decision should put litigators on notice that more courts are sticking to ESI protocols, encouraging collaboration, and requiring compelling evidence when the parties cannot agree to a deviation.

Mobile Equity Corp. v. Walmart Inc., No. 2:2021cv00126 (E.D. Tex. 2022)

In this patent infringement matter, the parties heavily debated production of Slack channel data, Jira documentation, and additional source code information. Plaintiff filed a motion to reopen a hearing on their previous motion to compel Defendants to produce this ESI, which the court granted. The judge made it a point to mention that Defendants uncooperative attitude towards full production was concerning – specifically with the source code data. Regarding the 40 slack channels at issue, the court directed the parties to meet and confer to narrow the Slack list in order to balance the burden.

The major takeaway here is that the number of relevant ESI sources will only continue to multiply and litigators need to be prepared. Remote working trends and emerging technologies are changing the nature of litigation and those that do not adapt can face case delays, disgruntled clients, sanctions, and negative outcomes. In today's world it is crucial to anticipate all data types as fair game, be ready to alter workflows, and increase collaboration with opposing counsel to reach proportional solutions.

Raine Grp. LLC v. Reign Capital, LLC, No. 21-CV-1898 (JPC) (KHP) (S.D.N.Y. Feb. 22, 2022)

This was a trademark infringement case where the parties could not agree to certain facets of their ESI protocol prior to moving forward with discovery. A major point of contention was the scope of search terms used. The parties could not agree on search term limitations and modifiers, so this issue had to go before the court. The court noted that it had broad discretion to manage the eDiscovery process and weighed in on how the search terms should be crafted to best capture all relevant documents while remaining proportional.

This ruling has a few key takeaways. First, it demonstrates the value of thoroughly debating ESI protocols before getting in the thick of production and review. By taking time to think through potential issues and bringing disputes to the court at an earlier stage, the parties will have more clarity going into the process and avoid extra costs and delay. Second, it illustrates a longstanding trend of search term issues resulting in proportionality debates. While not addressed here, it will be interesting to see if using TAR or other advanced workflows upfront can help lessen the number of proportionality disputes in the future.

Fast v. GoDaddy.com LLC, No. CV-20-01448-PHX-DGC (D. Ariz. Feb. 3, 2022)

A central issue in this case is when spoliation sanctions are appropriate with ephemeral messaging applications. In this employment discrimination case, plaintiff was terminated by defendant employer and filed suit claiming sex and disability discrimination. The defendants filed a motion for sanctions for failure to preserve numerous sources of ESI including emails, Facebook posts and messages, cell phone data, and Telegram messages. The Telegram issue is of particular interest as ephemeral messaging is currently a hot topic. While still in Defendant's employ, the plaintiff was getting assistance from a coworker on retrieving Slack data for potential litigation. The pair later talked about this matter over the ephemeral messaging application Telegram, which Plaintiff tried to conceal by failing to preserve the Telegram messages and deleting Facebook messenger exchanges referencing their chats over Telegram. The judge granted the motion and imposed adverse inference sanctions, attorney's fees and costs, forensic review of devices, and additional subpoena allowances.

Ephemeral messaging is still a developing topic when it comes to business functions so litigators should pay attention to how courts handle discovery disputes in this space. Here, the judge

made it clear that parties should never conduct conversations over these platforms when the duty to preserve arises. It is also important to understand when this duty arises, as it can be long before filing suit and will be based on the party's actions. Here, early gathering of information and retaining counsel for severance negotiations were triggers to preserve and communicate cautiously (even two years before filing this suit). While this does not mean that ephemeral messaging cannot have benefits in the workplace, once litigation is on the horizon these types of data exchanges must cease.

Another key takeaway from this case is the importance of counsel quickly implementing legal holds and ensuring key evidence is not lost. Many would think this would no longer be an issue, but emerging technologies keep this topic at the forefront and present new obstacles to consider. More data sources are harder to capture, can disappear, or may be subject to retention policies without being saved. Here, the judge placed some responsibility on plaintiff's counsel in this feat and stressed the danger of allowing clients to preserve in place without copying or moving the data.

Conclusion

These cases clearly illustrate that courts are encouraging parties to cooperate, be more proactive, and really think through their ESI protocols. Courts are not afraid to levy harsh sanctions to put litigators on notice of acceptable behavior and expect them to have a handle on emerging technology obstacles. It will be interesting to see how these trends continue to unfold this year (as these issues are still developing) and what new battles come to the table that keep eDiscovery professionals on their toes.

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 State of U.S. Data Privacy – 2022 Review and 2023 Predictions

Will the U.S. ever pass a comprehensive data privacy law? This question has long gone unanswered. With more states passing and considering legislation, the nation is left with a patchwork approach to privacy regulation.

This creates gaps and uncertainty regarding how to handle personal data, as many business activities cross borders. Add global obligations on top of this and it becomes very difficult to effectively manage compliance obligations. Data privacy is dynamic and will continue to be one of the most important areas to monitor, so it is important to grasp what happened last year and anticipate what is on the horizon.

New State Laws

In 2022, two more states passed data privacy legislation with Utah and Connecticut joining the ranks of California, Colorado, and Virginia. With how long the legislative process generally takes, it is impressive that five robust laws passed in the short time span of four years. This illustrates just how important privacy protection is in the digital age as there is much more potential for threat actors to intercept sensitive information. Here are some key features of these laws:

- **Utah Consumer Privacy Act:** This law grants similar rights to consumers regarding personal data such as the right to access, delete, and opt-out of sales. It also delineates separate categories for personal and sensitive data, has no private right of action, provides a 30-day right to cure period before enforcement, and places controls on processing activities such as notice and security obligations.

What makes the Utah law unique is that it is the most business friendly amongst the five states. Provisions that make is less restrictive include the inability for consumers to correct erroneous information; no requirement for organizations to perform data protection assessments, cyber audits, or risk assessments before engaging in riskier processing activities; absence of consumer appeal process; and an opt-out process regarding sensitive data collection as opposed to the opt-in mandates in other states.

- **Connecticut Data Privacy Act:** Many state bills incorporated provisions from the Washington state bill (that never passed), which make compliance easier by taking a less onerous and mandated approach. This has become known as the "Washington-Virginia model" as Virginia was the first state with these featured to successfully become law. Colorado and Connecticut have followed suit.

The Connecticut law also does not grant a private right of action and incorporates standard consumer rights such as accessing, deleting, and opting out of sales involving personal information. A unique feature of the Connecticut law is that while there is a right to cure, this sunsets on Jan. 1, 2025, and after that the attorney general has sole discretion to offer a cure period when a violation occurs. Other key components include strict limits on data collection/usage and the requirement that consumer consent be unambiguous.

So how do these two new laws stack up? There are several overlapping features in all five laws such as application across state borders and similar consumer rights. However, the departures make each unique and add another layer to compliance. A best practice is to understand how the laws diverge even when obligations appear to be similar. For example, although there is a right to cure in each state law the timeframe to do so differs. Compliance teams should also take note of how definitions vary and exemption language, as this

will affect what data is covered. These are small considerations that could have detrimental consequences if left unaccounted.

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. If and until a federal standard emerges, organizations must have personnel dedicated to privacy compliance and alter approaches based on which law applies. The Virginia law and California's Privacy Rights Act (which supplements the current California law) both became effective on Jan. 1, 2023. The Colorado and Connecticut laws are effective this July, and Utah this December.

Status of Federal Legislation

The federal government has been regulating data privacy in a piecemeal fashion through established legal frameworks like healthcare and credit reporting laws or Federal Trade Commission enforcement. A prediction from early last year was that more privacy laws and reliance on digital platforms may accelerate the creation of a new federal privacy framework. Some progress has been made on this front, but whether a comprehensive federal standard will materialize still remains unclear.

In July 2022, the American Data Privacy and Protection Act went to the House of Representatives. However, two clauses have been highly debated – one granting a private right of action and another allowing preemption of existing state privacy laws. For preemption purposes, there are current exemptions for sixteen state law categories including general consumer protection and data breach notification laws. While movement has been slow, many view this bill as non-partisan so lawmakers may continue to work through these issues and find a solution. In the interim, there are several ways this could play out in the states. More states may work vigorously to pass their own laws while others may be more apprehensive due to the possibility of a unified standard. A very real trend this year could be new bills containing provisions included in the proposed federal law, as this would lessen the effects of preemption in the future.

Additional 2022 Updates

Although only two new data privacy laws passed in 2022, legislators in nearly 30 other states considered bills that offered varying degrees of consumer protection. Some may be reintroduced during the 2023 session in addition to any new bills in the works. This sets the stage for even more state laws to pass this year. It will be interesting to see how they compare to the five currently on the books. Will any other states allow for a private right of action? Will future bills take Utah's more business-friendly approach or follow the Washington-Virginia model? Or adopt the Uniform Personal Data Protection Act? This is flexible model law based on tort instead of looking at data as consumer property. These are a few developments to watch.

Privacy was also a trending concern in other areas last year, which illustrates just how important this topic is to the nation. First, there was a wave of state bills similar to the Illinois Biometric Privacy Act. They aimed to regulate how organizations collect, use, safeguard, handle, store, retain, and destroy biometric data. While none passed, some are still pending this year. Also, monitor whether states with biometric laws that lack a private right of action decide to amend their laws if more BIPA-like ones begin to pass.

Second, in June, the New York Supreme Court adopted CLE requirements mandating attorneys to obtain one hour of credit every two years on the ethical obligations, technology, or practice considerations relating to cybersecurity and privacy topics. Including privacy emphasizes just how important protecting personal and sensitive information is in today's world. 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

What happens on the federal front these next few months will set the stage for the rest of the year. Regardless, organizations subject to any state laws becoming effective this year need to implement the appropriate changes to avoid violations and operational interruptions. Keep monitoring all data privacy activity in the U.S. and abroad, as anything is possible with such a dynamic landscape.

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.

Is the EU on the Cusp of Pioneering AI Regulation?

Artificial intelligence (AI) is a fascinating tool in the modern world. It can suggest products based on a person's search history. It can recognize faces to unlock a device. It can help recruiters pick the best candidate to fill a position. It can cull datasets down significantly for a case or investigation. And so much more.

While AI has revolutionized many aspects of business and personal life, many have expressed concerns over inherent bias. Humans need to train AI tools before deployment, which can create vulnerability to bias and prejudice. If this occurs and no one ever challenges the technology, then it becomes difficult to explain decisions and opens the door to reputational harm and legal liability.

While there has been some patchwork regulation in countries like the U.S. and China, there are no broad laws on the books. The EU has taken a groundbreaking step via the Artificial Intelligence Act, which is currently deep in the negotiation process. It was introduced in April 2021 and had been moving through the legislative process these past two years.

Right now, the European Parliament is expected to vote in the spring and the law should be approved into law this year. The U.K. also has released a policy paper on AI taking a different approach. It is crucial to understand what these laws would change and start preparing for compliance, as this will set the stage for other countries to follow suit.

The EU's Artificial Intelligence Act

The goal of the EU's AI Act is meant to promote transparent and ethical AI usage while safeguarding data. While it is not in final form yet, it is nearing the end. Here are key features of the proposed law:

- The definition of AI covers all software developed with machine learning, logic-based, knowledge-based, and/or statistical approaches. Organizations that develop or use such software in the EU would be subject to liability.
- AI tools will fall under four categories: unacceptable, high-risk, limited risk, and minimal risk. Unacceptable systems

such as social scoring used in the public areas would be banned under the law. The regulation mainly focuses on those falling into the high-risk category. This includes AI used for employment, law enforcement, education, biometric identification, and more.

- AI providers have the highest burden. Key obligations would include a prior conformity assessment before putting a tool into the market; creation of a risk management system to target bias during the design, development, and deployment that carries through the entire usage lifecycle; cybersecurity requirements; recordkeeping; human oversight at every step; quality management; creation of strong AI governance frameworks; and public registration.
- The term AI users would include individuals and organizations that use AI under their authority as opposed to end-users. Recruitment agencies are a prime example. Responsibilities include training with relevant data, monitoring, recording, data protection impact assessments, and strong AI governance frameworks.
- Penalties are high, and currently include up to 30 million euros or six percent of the breaching organization's global revenue.

As this continues to move through the process, it is important to take note of any changes or additions. Lawmakers have

expressed concerns over how it will regulate biometrics and ensuring there is flexibility embedded in the law due to AI's dynamic nature.

Proposed U.K. Approach

The U.K. policy paper on AI governance and regulation came out last summer. It also strives to promote transparency, security, and fairness. However, it departs from the EU regulation in many aspects by focusing more on innovation via a sector-based approach.

Put simply, while there would still be standards to follow, each agency would regulate AI usage in their specific sector. This is designed to avoid too much regulation and account for differing risks amongst industries. The U.K. regulation would be tech agnostic focusing on outcomes and whether systems prove to be adaptable and autonomous, as these types of AI are unpredictable and have more inherent risks.

Although this would give U.K. regulators flexibility, there would be core principles to follow when governing an organization's AI usage:

- Ensuring safe AI usage
- Ensuring the system is technically secure and functions as designed
- Transparency and explain ability
- Embedding fairness considerations into the system
- Designating a legal person as responsible for governance
- Creating clear protocols around redress and contestability

A white paper further detailing this topic was expected to come out late-2022, but that has not yet occurred. When this is released, it will provide further insight as to whether the U.K. will move forward with official regulation and provide a better sense of the timeline.

Next Steps

AI will continue to integrate into society in a multitude of ways as technology advances. Regulation in this space will help alleviate fears of bias, protect data, encourage innovation, and explain the decision-making process. But will this type of regulation trend globally like what happened with privacy regulation after the GDPR passed? Will the EU set a global standard, or will there be more movements in the U.K. or other countries like China who have already tested the waters on a smaller scale? Only time will tell. Right now, monitoring legislative developments and getting a jumpstart on compliance initiatives is the best way to prepare.

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 Increasingly Complex World of Competition Review

Regulatory enforcement agencies are changing their approaches when it comes to competition, and that is now having an effect on the U.K. and European markets. Data and technology underpin the evolving strategies, and it is expected regulators will ramp up scrutiny and expect increased cooperation while investigating merger control, corporate leniency programs, and beyond – even in industries that have historically been at lower risk of investigation.

Merger Control

There is an identifiable pattern of increased intervention by competition and antitrust regulators. More deals are being investigated, subject to secondary requests, or litigated. This especially rings true in North America and Europe. Trends emerging in several countries include increased scrutiny over industries previously viewed as being low risk.

Deals involving dynamic markets where innovation is critical are facing heightened scrutiny in many areas including the U.S., U.K., and EU. This includes transactions involving digital platforms, healthcare, and pharmaceuticals. While private equity purchasers in these industries are not usually subject to regulator scrutiny, this is predicted to change – particularly in the case of cross-directorships. While there is more coordination among regulators than previously identified, divergence is still present. All of this makes the process longer and adds complexity to substantial compliance.

Dawn Raids

Digitization continues to influence many business and legal processes, including the way authorities around the world conduct so-called "dawn raids." Hybrid raids (i.e., in-person and remote collections) are also on the table now due to the fact that pertinent information lives on devices kept at the residences of remote workers. It is imperative that organizations are prepared for, and can respond to, unannounced inspections at all levels of the company regardless of where their office is located. Corporate employees need to understand the obligation to preserve and produce written communications during an investigation.

Organizations should take steps to be prepared for dawn raids and develop partnerships with outside providers to help with this feat. Company-wide dawn raid plans should include communication charts, risk avoidance policies, checklists, data hygiene, and tech usage protocols. Consider developing or updating policies in partnership with external counsel and document management experts. All this will foster thorough response efforts and limit the potential to overshare data with regulators.

The Expansion of Data Requests

Although large data requests have always been a feature of the U.S. merger control landscape, they are now becoming increasingly common in the U.K. and EU as well. The exploding volume of data, combined with the increase in regulatory scrutiny, introduces the "double whammy" of more data and the likelihood of it being subject to discovery requests. Remote work only adds to the digital footprint and presents collection challenges when workers conduct business over personal devices. Teams can be proactive by using preventative solutions to help with compliance efforts during an investigation and understanding regulator preferences in regard to technology and workflows.

When working with competition authorities on multi-jurisdictional matters, workflows in parallel investigations must be monitored to ensure consistency. A global response will

drive efficiencies in the review and disclosure process while also ensuring that privilege is protected and legal obligations are met. This is where using a combination of tools, such as artificial intelligence (AI) and search terms, can be beneficial. Legal counsel, partnering with legal technology providers, can train algorithms to identify privilege.

Leniency

With an increased focus on the ethical and responsible behavior of corporations, there have been recent changes regarding leniency procedures. Some regulators incentivize early action through the possibility of material reduction in fines. The U.S. Department of Justice recently revamped its leniency program to include accelerated self-reporting relating to anticompetitive behavior. The U.K. Competition and Markets Authority is also considering leniency reform and encourages self-reporting.

There have been recent developments in the role of advanced analytics and AI tools that can identify conduct that may violate competition laws. Organizations can use these as monitoring tools to be proactive and apply for leniency. Settlement agreements with regulators may even require an active monitoring component to identify potentially illegal behavior. As part of an organization's defensibility efforts, it is vital to work closely with legal advisors to understand risk profile and identify any areas that require further intervention, then use AI and predictive tools to assist with preventative and proactive audits. Also, companies should take into account data privacy regulations during this process.

In sum, data and tech sophistication are the underlying drivers of these trends. Regulators will continue to increase scrutiny and expect cooperation during investigatory processes. Retaining experts in document management and legal technology who understand data mapping and structure, have the right technology options, and knowledgeable consultants is key to remaining compliant.

On Nov. 17, 2022, Epiq and The Lawyer co-hosted a webinar to discuss how these issues are playing out in the U.K. and European markets. To listen to this webinar, 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.

It's Time to Blow the Whistle on Deficient Cyber Reporting Programs

What exactly is cybersecurity whistleblowing? That is a question that all organizations should be asking, but the answer is not a simple one. According to the Merriam-Webster dictionary, a whistleblower is defined as an 'employee who brings wrongdoing by an employer or by other employees to the attention of a government or law enforcement agency.' While whistleblowing is familiar in situations such as unsanitary working conditions, hazards, and payroll fraud - cyber is a fairly new territory. Now is the time to understand what this actually encompasses in order to take appropriate steps to combat security threats and close gaps before regulatory involvement.

Managing cybersecurity concerns and the possibility of whistleblowing needs to be included in cyber readiness initiatives, but also embedded in company culture. Having the enterprise take a teamwork approach to cybersecurity will increase awareness, provide a clear reporting mechanism to voice concerns, and control uninformed whistleblower claims. But what does this look like and where should CISOs and legal begin? While there is not a "one-size-fits-all" solution, there are fundamental steps to take that will make it easier to spot imminent security threats, manage cyber resources, and streamline internal investigations.

The Dilemma

New digital threats are constantly surfacing. Organizations have to balance these threats against budget constraints, resources, regulations, and data indicating attack probabilities. A breach can lead to serious legal and reputational consequences. Clear information governance, incident investigation, and breach response plans are important to limit the fallout. However, even when having strong protocols in place there needs to be additional measures to facilitate cyber awareness. Without proper communication on cyber controls, reporting procedures, and companywide responsibilities – an organization opens the door to claims that could be avoided or remedied prior to regulatory involvement.

Imagine this scenario. An employee believes there is a serious security gap and reports it to someone within the organization. Turns out, this was the wrong person to contact

and it fell between the cracks. Failure to address this issue results in a breach and regulatory involvement or legal liability ensues. Going in the other direction, say the perceived gap actually was not a threat but the employee felt unheard and filed a formal complaint or called their employer out on social media. Either way, harm will ensue that could have been avoided. Had the organization implemented better communication regarding reporting procedures, this could have been investigated and resolved internally.

Maintaining cyber programs where reporting procedures are clear and routinely communicated is crucial. Also include whistleblowing protections in company handbooks and as a part of cyber training so everyone knows their rights, as there are absolutely times when these measures are warranted. Several regulators have recently increased protections and are incentivizing cyber whistleblowers. The range of behavior covered is wide and includes things such as breaches and security vulnerabilities. To balance all of this, company culture needs to evolve.

Changing Culture

While there is always the likelihood of uniformed and unsubstantiated complaints, this can be counterbalanced with increasing cyber awareness within the enterprise. Make it known that protecting company data is every employee's responsibility and there are procedures in place to accomplish

this feat. In turn, the right complaints will get to the right places and there will be solid checks on cybersecurity to achieve the ultimate goal of keeping data safe.

Here are three hallmarks of a solid plan to elevate cyber hygiene within an organization.

Enhance cyber training programs

Oftentimes people that report problems to regulatory agencies or the public often do not have all the information relating to business risk decisions or complex technologies involved. The resulting investigatory response and reputation repair will utilize a lot of resources. This reality needs to be offset with valuable education that will promote transparency and expand cyber knowledge for everyone in the organization. This should be included past onboarding and be embedded into daily activities via mandatory training, open forums, cyber alerts, simulations, and other educational opportunities. Also ensure that managers regularly talk about cyber responsibility to their teams and how to report suspected issues via the appropriate channels.

Offer a reporting hotline

Having a hotline set up through a third-party is a solid investment to help manage cyber complaints while also providing the added benefit of employees feeling more comfortable to report. Hotlines are often part of a larger initiative, so if cyber complaints are not included in a current agreement it is a good time to think about the benefits of expanding these capabilities.

Have detailed protocols for handling complaints

There will likely be several ways that cyber reports occur, even when a separate hotline or IT process are in place. Other avenues could include direct managers, HR, and legal. Everyone in these roles – and throughout the entire organization – should know where to escalate reports. Then, the appropriate team can sort through the reports and determine which issues are actual threats, everyday IT issues, or instances of whistleblowing. Risk analysis and legal obligations will feed into these designations. Having policies around following up with individuals who report is also a good idea to keep decisions transparent and defensible.

Conclusion

There are two important takeaways here given the regulatory landscape and increasing importance of cybersecurity in business. First, organizations need to understand that cyber whistleblowing is a real possibility. Second, updating programs to address internal reporting gaps is critical. Tackling problems head-on results in quicker remediation and lower exposure risk. This also allows the organization to allocate resources to fix a security problem earlier on versus dealing with a larger investigation or reputational repair down the road.

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.

Is the Metaverse More Than Just Talk?

Everyone seems to be talking about the metaverse – how it's defined and still evolving into a standalone digital economy. But has there been any real progress as the metaverse positioning itself as the next iteration of the Internet? The short answer: not really.

Interestingly, the term metaverse was coined more than three decades ago in 1992 in the sci-fi book "Snow Crash," authored by Neal Stephenson. The book described the metaverse as an all-encompassing digital world running parallel to the real world. While that seems to be what the goal is presently, what will materialize long-term is unknown. The term metaverse is definitely a buzzword right now, but so was the term internet years ago. After use cases multiplied, adoption rose and the internet skyrocketed into the force it is today.

Currently there are several digital spaces that make up the metaverse. Progress has been made on the business front, but it is still in the very early stages. It will be years before it is used regularly across industries because trust takes time to build. The thought of transacting business in an immersive, three-dimensional shared virtual space is intriguing, but also daunting. But that does not mean organizations should not be thinking about how they can use the metaverse. In fact, now is the optimal time for forward-thinking companies to consider potential use cases.

Recent Activity

The metaverse sparked a lot of interest last year. Companies in the tech and gaming industries provided hefty investments to help build up the virtual space. Digital currencies and layered technologies are fueling this complex space. There are several immersive and social gaming options and concerts, such as Travis Scott, have even taken place in the metaverse during some of these gaming experiences.

Businesses in other industries have also started exploring options for transacting in the metaverse and some even opened up shop. This includes banks, retailers, and more. Marketing is a trending focus for organizations to promote their brand in a new space. For example, while retailers can make sales by offering outfits and accessories for avatars –

brand awareness also spreads when these retailers have space in the metaverse. In the legal space, several law firms have opened up but lawyers are not really advising clients yet.

One common theme for all of these endeavors is that they are in the infancy stage. Business and legal leaders would be wise to pay attention to how this space transforms over the next decade.

Potential Use Cases

There will be several opportunities to leverage the metaverse for business in the future as this space evolves. Think of the endless possibilities. Colleagues and clients can put on headsets and be taken directly to a space where they can interact with a person living across the globe just as they were in person. The interactions go far beyond what many have been doing over video chat the past few years, as they are much more realistic. Users can even maintain anonymity through their digital avatar if needed for a sensitive manner.

Big tech, gaming, entertainment, marketing, and retail will likely continue to dominate the metaverse for now. However, potential use cases for business outside of these are within reach. This includes industry conferences, internal meetings, client consultations, contract negotiations, vendor interviews, document review, and more. Once privacy and data security controls are more certain, medical visits could even be a use case for healthcare organizations. It seemed impossible that

doctor visits could occur remotely, but over the past few years this has become more common. Who's to say healthcare will not also be provided in the metaverse?

While more of the legal industry is starting to prioritize innovation, many still remain hesitant to jump on new tech trends until the risks are realized. Some leading law firms have already dipped their toes in the metaverse, but getting the whole industry on board will likely take a lot longer. If and when this occurs, the use cases are numerous. This includes client consultations and meetings, internal collaboration, metaverse courtrooms, depositions, ALSP partnerships, and document review. Additionally, client usage of the metaverse will drive lawyer education and adoption. This presents opportunities for new practice areas, advising clients on safe metaverse usage, and more.

Now is the time to watch if any of these business and legal use cases materialize and how widespread they become. Will metaverse endeavors be limited to innovation pioneers or will adoption spread quickly? Will certain industries continue to dominate and build up this space for the foreseeable future? The timeline and adoption trends are unknown. Anything is possible at this point and time.

Projected Risks

Many business and legal leaders will wait and see how metaverse risks are defined before making significant investment. The top three risk categories to consider are legal, cyber, and privacy.

Legal

From a legal standpoint, it is unclear which laws apply in the metaverse and how they will be interpreted. Will the metaverse need its own body of law or will current laws apply? Who has jurisdiction over a dispute? How will trademark disputes be handled? These are some key questions to tackle before transacting in the metaverse.

As with all new tech, there will undoubtedly be unique collection and review obstacles when data relevant to litigation or investigations resides in the metaverse. Preservation challenges will arise causing organizations to revamp their information governance programs to account for data storage in the metaverse. This will require an understanding of what data could be discoverable and how retention policies factor into protecting that data. Also anticipate collection obstacles that will require new workflows to obtain relevant data. Partnerships with providers that have the tech to collect difficult data will be key to remain compliant. Future court decision and regulatory opinions will be instructive on these issues.

Cyber

As the metaverse expands, hackers will look for any opportunity to breach information. Cryptocurrency payments and unsecured systems will be prime targets. Consulting with a cyber attorney or expert before storing data or transacting in the metaverse will be crucial. Consider implementing security-by-design models and placing extra controls to keep data safe. Also pay attention to the inevitable breaches that will occur in this digital space, as they will shine light on deficiencies and gaps to consider before setting up shop in the metaverse.

Privacy

An organization's data privacy program will need to translate to metaverse interactions. However, it may be trickier to determine which laws apply. Best practice for now is to operate as if the strictest applicable law applies. It may also be more difficult to comply with privacy obligations such as the right to access or deletion, so for now it may be prudent to limit which data is stored in the metaverse.

Conclusion

The metaverse is forming and it is hard to predict whether it will integrate into everyday life like the internet did so many years ago. Right now, many view it as a risky place to conduct business. Until this is proven true or false and best practices arise, adoption will continue to be slow. It is prudent to keep tabs on what innovators and industry competitors are doing in this space, as this can mold future business strategies. Legal, cyber, and privacy analysis will play a huge role on setting parameters and realistic expectations for what data should be stored in the metaverse and how to best protect sensitive information.

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.

A Note to CFOs From the Legal Industry

As economists debate whether the world economy is headed for a recession with a "small r," a "slowcession" or a "soft landing," CFOs are increasingly turning to the most common way to reduce cost - layoffs.

For most corporate functions, layoffs achieve the intended purpose of cost reduction. A notable exception is the law department, where headcount reductions can result in a cost increase.

Although in-house compensation varies significantly by industry, practice area and geography, the Thomson Reuters 2022 State of Corporate Law Departments report estimates the average fully loaded cost of a US senior in-house lawyer at $329,000. If that lawyer is laid off, has the company actually saved $329,000?

If the work that lawyer was doing has gone away due to an economic slowdown, then the answer is yes. However, because legal work and business activity are not perfectly correlated, it's very possible that much, if not all, of that lawyer's work will remain. Where does it go?

If that work is now outside the expertise of the law department, it will often go to a law firm which will cost more. The average billing rate for law firm partners in the U.S. is $728/hour (in the Am Law 100, that is a typical rate for an associate.) Let's conservatively assume that 1,000 hours of the senior in-house lawyer's annual workload cannot be re-assigned within the department and that the work requires partner-level attention. In that case, laying off the attorney will increase its costs by almost $400,000.

The issue is not just financial. If only 1,000 hours are sent to a law firm, then there will be a significant number of hours reallocated among remaining members of the law department. Consequently, turn-around times on customer contracts, legal or regulatory review of new products and other business-critical activities will slow down, which is the exact opposite of what a company needs when adjusting to challenging times. Furthermore, it's likely that some matters that should get legal attention will not, increasing the company's risk profile.

Of course, this does not mean a CFO should give a free pass to the law department. Law departments today are better equipped to manage costs than ever before due to the rise of the legal operations profession, the evolution of alternative legal service providers (ALSPs) and emerging, and increasingly mature, legal technology. Such technology not only drives efficiency, but it can also identify immediate cost savings opportunities such as compliance errors in outside counsel invoices.

Use, don't lose, your Legal Ops teams

Of concern to many of us who have been pushing innovation in the legal industry is the idea that legal operations teams will be seen as a 'luxury' that should be targeted in a cost reduction. Legal operations professionals are the drivers of process, transformation and technology adoption, in the law department – in tough times these are not luxury items. Quite the opposite.

It is exactly times like this when high performing legal operations teams can add the most value...if GCs and CFOs make them part of the conversation on how to reduce total cost (internal and external) for legal. Companies that significantly cut their legal operations team will look back on that decision and realize that it was a backward step toward the ultimate goal of transforming the legal function into one that delivers significant, measurable value and counterproductive to the short-term goal of cost reduction.

A key difference between any potential 2023 recession and the ones we saw in 2007-2009 is the wide array of mature, sophisticated solutions that law departments can utilize to measure, evaluate, and meet both the legal needs of the business and the cost demands of the CFO.

Our advice is to give your legal operations leaders the space to run towards these potential challenges and double down on efforts to create sustainable efficiency plans that focus on total cost and value. Let's embrace transformative solutions and continue to move the legal industry forward.

If you found this blog informative, you may enjoy reading Legal Ops Teams Targeted For Layoffs Amid Cost-Cutting 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.

More Businesses Using Biometric Data Means More Regulation

Biometric data continues to take up a massive amount of space in the digital universe. Fingerprints, facial scans, and voice recognition are staples of modern devices and are regularly integrated into business models.

Think about how biometric technology plays a role in tools for employee identification, automated voice assistants, virtual try-ons, account sign-on verification, event access, and social media filters, to name a few. Organizations may collect this data not only in the regular course of business, but also during discovery for a lawsuit or investigation. As a result, the U.S. has experienced more pressure for regulation in recent years. This body of law continues to evolve so do not forget to turn alerts on for biometric updates in the legal space to keep on top of pivotal decisions and legislative trends.

Recent Case Law

Illinois was the first state to directly regulate biometric data through the lens of consumer privacy in 2008 via the Biometric Information Privacy Act (BIPA). This strict law applies to how organizations collect, use, safeguard, handle, store, retain, and destroy biometric consumer data and has been a groundbreaking piece of legislation not only in Illinois but throughout the nation.

Private lawsuits are authorized and prospective plaintiffs do not need to show actual harm to establish standing. A procedural violation is sufficient to file a BIPA lawsuit, including class actions. This has resulted in a flurry of litigation since its inception fifteen years ago, with some pivotal decisions and trends materializing the past year. Take a look below:

- The first BIPA class action went to verdict in October 2022. In Rogers v. BNSF, the issue was an employer collecting biometric data without employee consent or notice of data retention policies. The unique part of this case is that the employer did not directly violate BIPA, but it was instead a third-party that collected and used this data in violation of statutory mandates. The jury quickly entered a verdict in favor of plaintiffs finding reckless/intentional statutory violations 45,600 times. Each fingerprint scan counted as a violation and constituted a separate $5,000 award. The court entered total damages in the amount of $228 million. This verdict puts employers on notice that they can face vicarious liability for the unlawful actions of vendors and be subject to high monetary penalties.
- On Feb. 3, 2022, the Illinois Supreme Court in McDonald v. Symphony Bronzeville Park ruled that the worker's compensation statue does not preempt BIPA. This eliminated a key employer defense and continues the trend of courts broadly interpreting this law. Further widening the floodgate potential in turn raises exposure risk as BIPA damages can be quite high.
- Trends include lawsuits centering on facial recognition data collection and targeting retailers. Examples are virtual try-ons, AI-enabled voice assistants, and similar technologies. Courts are also interpreting facial scans broadly, such as encompassing bystanders captured on outdoor video from a private residence.
- Case law dictates that it does not take much to proceed past the pleadings stage. Many motions to dismiss have proved unsuccessful and cases proceed to the discovery phase.
- On Feb. 2, 2023, the Illinois Supreme Court rendered a pivotal decision regarding statute of limitations. BIPA does not provide a limitations period, so the Illinois Code of Civil Procedure governs. There was debate regarding whether

provisions applying a one-year or five-year limitations period applied. The court ruled that the five-year catch-all provision applies to all BIPA claims.

- On Feb. 17, 2023, the Illinois Supreme Court came down with another key ruling confirming that plaintiffs can bring claims for each time an organization unlawfully collects or discloses their information. It was a close call and the majority recognized the extreme liability this could place on defendants and left discretion to the trial courts on how to enter damages. The Court attributed the ruling to the plain language of the statute and said that lawmakers would need to make any changes in this regard.

There are notable underlying themes. Courts are continuing to interpret BIPA broadly to put organizations on notice about unacceptable data hygiene practices. It does not take much to establish a cause of action, the potential plaintiff pool is wide in class actions, statute of limitations is longer, damages can be massive, and liability is expanding to third-party actions. The explosion of BIPA litigation seen over recent years will not slow down anytime soon, so organizations need to regularly evaluate their exposure risk and take steps to mitigate proactively. Failure to do so could result in BIPA-related litigation costs and monetary liability.

Other States

Texas and Washington have similar biometric laws on the books, but do not allow for a private right of action. It is important to know the similarities and differences between the three laws, but enforcement in Texas and Washington has not been anywhere near BIPA level due to the absence of this right to sue.

In 2022, there was a wave of state bills that signifies more states are trying hard to get a biometric law on the books. While none passed, as of January 2023 two bills have already been introduced in the new legislative session (Maryland and Mississippi). There is expected to be another flurry of biometric bills throughout the country this year as the sessions progress.

What is interesting about the 2022 bills is that they fell into several different buckets. Some were straight BIPA copycats. Others were hybrid bills incorporating both BIPA protections and those found in current consumer privacy laws. The third category was more targeted at facial recognition and voice data regulation. At a local level, Baltimore and Portland have already successfully passed laws targeting facial recognition in the private sector.

It is crucial to monitor what model prevails if and when more state bills pass into law. What will be especially interesting is whether any include a private right of action pass and how the resulting case law will mirror or differ from interpretation of the Illinois law. Also, whether more states decide to focus on targeted laws since facial recognition is currently the hot topic.

Conclusion

So, what should litigators and organizations handling biometric data be doing this year? Ramping up compliance efforts, monitoring relevant court decisions, and tracking legislative process outside of Illinois will be key. While BIPA can apply outside Illinois, new state laws that pass would add to the dominance of biometric litigation.

The correlation of more biometric data collection and increased regulatory attempts nationwide signifies the importance of how data trends drive legal action. Facial recognition will definitely be a continued focus and new trends will undoubtedly materialize. Organizations must understand their risk with biometric data collection so they can close gaps and stay ahead of the curve.

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.

Minimizing Data to Minimize Exposure: Information Governance and Data Security Overlap

How important is it for organizations to keep track of their data footprint? The Federal Trade Commission (FTC) thinks this is crucial. On Jan. 9, 2023, the FTC finalized a consent order following a breach. The order was pending since last October. While there were several components, the part involving data minimization is compelling.

Every organization subject to FTC jurisdiction should take note of how the requirements influence information governance and data security practices going forward. Compliance is an ever-growing space and more regulators are emphasizing appropriate security priorities in the digital ago, so failure to get on board can result in investigations and liabilities.

The Details

In 2020, the online alcohol marketplace Drizly underwent a large data breach that put the personal information of roughly 2.5 million consumers at risk. The cause was due to security failures that the organization was made aware of two years before the breach when a prior incident occurred. While Drizly declared to have sufficient security measures, investigation showed that this was untrue. Violations included absence of basic safeguards, use of unsecure platforms, and insufficient threat monitoring. A hacker was able to access an employee account and company database and steal corporate logins and personal customer data.

The FTC took action against Drizly and its CEO for this breach and entered a consent order. During the public comment period, there were no substantive changes proposed and the order passed with a unanimous vote. Many of the requirements focus on data minimization practices to limit the potential of a future breach resulting from improper data hygiene:

- Stop collecting or storing personal information unnecessary for business needs.
- Destroy any unnecessary data previously collected and send report documenting this to the FTC.

- Publish a retention schedule on their website that details why the company is collecting certain personal information, retention periods, and related business need for retention.

Other requirements under the order include having a comprehensive security program with numerous safeguards including multi-factor authentication and technology that helps accomplish data deletion; having third parties perform security assessments biennially for 20 years; and, the CEO personally having to implement a comprehensive security program at future companies if certain conditions are met relating to job title and consumer data collection.

The Significance

This enforcement action is significant because it spotlights the importance of implementing preventive security measures to limit breach potential. The interplay between strong information governance practices and safeguarding data is continuing to deepen. Organizations should make data governance a continuous effort to effectively protect sensitive data.

While data collection and storage are absolutely necessary for business purposes, it can be a slippery slope. Data continues

to generate at an alarming rate and there is no slowdown in sight. The more data an organization keeps, the more data there is to fall victim to a potential compromise. The type of personal information out there also makes a breach even more serious, as it is no longer just someone's name and birthday. Now, many businesses collect highly sensitive identifiers. Think facial scans, fingerprints, geolocations, user credentials, and more. Hackers are waiting in the wings to get this information and perpetrate fraud or other harmful activities. The FTC recognizes this and expects the trend of requiring data minimization in matters like this will not die down.

The Solution

Data minimization requires ongoing effort and should be a staple in information governance programs. The first step is to ensure that information security and data privacy obligations are intertwined with these efforts. To have appropriate security policies and procedures requires a well-crafted data governance framework to properly manage valuable information and minimize risk. When organizations have a deep understanding of their data footprint, it becomes easier to understand what needs to stay and what can go. Then, they can implement the correct policies and solutions to achieve goals such as minimization and retention management.

This can be a daunting task to take on alone due to time management and compliance concerns. Look for a provider partner that offers a range of technology-enabled and consulting services for planning, executing, and managing data minimization. The right partner will not only have the tech, but also the people who understand the regulatory and reputational aspects that feed into good data hygiene. Tapping into such expertise will help teams understand their internal and external risk exposures and what steps to take to maintain good data hygiene and actively monitor their data footprint.

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.

Generative AI and Business: The Basics and Benefits – Part 1

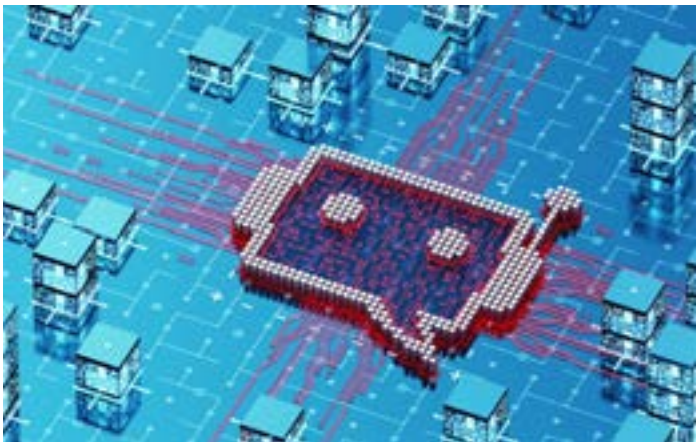
Is generative AI just a new buzzword or will it play a meaningful role in business? Legal is one industry that should take note, as more organizations are prioritizing innovation. Many firms and corporations have already realised the value of technology powered by artificial intelligence (AI) that can detect relevant data and produce better outcomes.

AI tools are regularly used for document review, settlement evaluation, litigation analysis, internal investigations, regulatory compliance, and strategy decisions. This has proven to be transformative and drive better results at a faster pace. Improved outcomes build trust, which has started to slowly turn an industry known for hesitation into one that embraces innovation. But will this pattern ring true with generative AI? Read on to get a deeper understanding on what generative AI is and why the legal industry should care about this trending technology.

The Scoop on Generative AI

Generative AI operates off of deep learning models combining algorithms allowing for quick content creation in response to user input. It has actually been around since the 1960s when the first chatbot emerged, but while this is not considered "new" technology, recent advancements have made these tools more popular. The tech behind this? Transformer machine learning has made it easier to train large datasets leading to more comprehension and robust responses. As a result, new language models have surfaced that can make deeper connections with words and phrases resulting in compelling content.

From the ability to answer questions in a conversational manner to producing detailed images and video, generative AI has caught the attention of many over the past few months. Users are fascinated by how easy it is for ChatGPT to understand a command and respond in seconds – from answering simple questions to writing poems and even passing standardized tests, including the Bar and MCAT. Or how Stable Diffusion can produce a high-quality realistic image just based off a text description. These are just a few examples of trending generative AI tools that are out there.



An important question to ask is how generative AI differs from other tools that legal professionals and their clients are already using. Predictive coding tools such as TAR are widely accepted for identifying key documents and themes early on in a matter and efficiently managing the assessment and review of data. These tools have matured since introduction, as now some can perform sentiment analysis and pattern processing. There are even portable AI models available for a variety of matters. AI is also used in contract management and analytics, privilege review, privacy law compliance, and more. Similar to other types of AI, training is necessary for generative AI to grasp natural language. The difference lies in the underlying algorithms and what the technology outputs. Other AI tools (such as TAR) process data inputted to help classify, detect patterns, and make decisions when reviewing documents. Generative AI creates new content and chat answers based on prompts.

Looking Ahead

How will generative AI integrate into business and legal processes? This is something to be curious about. It is important to be proactive with tech trends, as demand can materialise quickly. Balancing the benefits and risks will help lawyers make informed decisions regarding use cases, remain innovative, and be better equipped to advise clients.

Here are four reasons the legal industry should monitor generative AI developments:

1. The potential use cases are plentiful. Template creation, eDiscovery, motion drafting, contracts, and research are a few that could trend in the coming years. Innovation is taking the legal industry by storm so evaluating emerging technologies is critical to remain competitive.
2. Clients will be using this technology and will have questions. Keeping apprised will provide the ability to counsel on usage, policy drafting, and risk management.
3. Ethical obligations are always heightened for lawyers, which means this needs to be an integral part of risk analysis. Some generative AI can open the door to waive privilege and violate the attorney-client relationship. Consider these factors before inputting confidential information in a generative AI tool.
4. New tech always raises cyber concerns, as threat actors look for any way to compromise data. If using generative AI, organizations must account for cyber risk and include any relevant information in breach readiness initiatives. Also look out for content created by threat actors for phishing expeditions, as access to a generative AI tool could help create more realistic attempts.

As use cases expand and studies materialize, it will be easier to realize true benefits and perform risk analysis for generative AI in business. In some instances, this could prove to be another tool in the tech toolbox that can improve efficiency and control costs. Check out next week's blog from the Epiq Angle for part two of this topic that will take a deep dive into ChatGPT – what it is, how it works, and limitations the legal industry must consider.

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.

ChatGPT: What's the fuss?

What's all the buzz around ChatGPT? This new chatbot, powered by an artificial intelligence (AI)-based language model called GPT-3, has caused a lot of waves lately in our industry. Users can ask questions about anything, and the bot will engage in conversational dialogue with very organized and succinct responses that are often indistinguishable from human-generated output.

GPT-3, from the OpenAI foundation, is part of a family of AI models known as Large Language Models (LLMs). This is an area of research (Generative AI) that is moving quickly, with the recent announcement of GPT-4, and similar LLM's such as Google's LaMDA also making the news. How well the ChatGPT bot understands language is remarkable and seems superior to any other LLM currently available to the public, although it is important to understand that it is specialized and trained on a far smaller subset of data than GPT-3 itself. Users of ChatGPT can provide feedback on responses which is used to further tune the application. General ChatGPT usage is currently free during the initial phase with advanced membership options available for a fee.

People are already starting to use ChatGPT to get answers to everyday questions and even for some research purposes. To test capabilities, users have even asked ChatGPT to take standardized tests. While it did not perform for all, it did achieve passing scores for some tests including the Uniform Bar Exam (UBE) and the Medical College Admission Test (MCAT).

As with any emerging technology, it is crucial to balance both benefits and risks when utilizing this technology for business purposes. From a legal standpoint, it is necessary to understand the unique collection obstacles and review benefits this technology can offer for eDiscovery purposes; other use cases for lawyers and their clients; and how ethics may factor into any LLM based endeavor.

Putting ChatGPT to Work

With new technology trends, concerns often surface about whether certain tools will replace humans – especially in the legal industry. The sentiment applies here, as there have

already been questions about whether GPT-3 and other similar AI language models could take over the human function for jobs that still require an element of oversight. In the eDiscovery space, could LLMs review and flag responsive documents without needing human oversight? Or does this seem way too far-fetched? Before answering that question, check out what quickly came back when we asked ChatGPT to write a blog about ChatGPT and eDiscovery:

ChatGPT, a cutting-edge language model developed by OpenAI, has quickly gained recognition for its ability to process and understand natural language. As a result, it has become an invaluable tool for a variety of industries, including the legal sector.

In the field of eDiscovery, the use of ChatGPT has revolutionized the way that attorneys approach the discovery process. With its advanced language processing capabilities, ChatGPT is able to sift through massive amounts of data, including emails, text messages, and social media posts, in a matter of seconds. This allows attorneys to quickly identify relevant information, saving both time and money.

This is just a third of what the chatbot actually came back with. It also included information about the key advantages of using ChatGPT in eDiscovery and final thoughts on how use cases for language models will increase in the future. At first glance,

it makes sense why some analysts believe this tool could replace humans in higher level roles. However, it is important to recognize that although language models such as GPT-3 may prove beneficial – limitations exist.

Understanding the Limitations

While the ChatGPT bot and AI models like GPT-3 are innovative, there are still risks and limitations to account for before using them for business purposes. Take the example above. While it came back with a lot of helpful information and even formatted the text like a blog – what did ChatGPT miss? It did not provide any information about the tool's training history, limitations, risks, or ethical considerations. These are all things that lawyers and their organizations have to consider before using new technology so they can make an informed decision and adequately represent their clients.

Here are five key limitations to consider as advanced language models continue to emerge and evolve. This will help balance the benefits and risks so organizations can make educated assessments about appropriate use cases.

1. Lawyers will still need to make some relevance and privilege determinations if using LLMs for litigation or investigatory review functions. There is currently no strong evidence that this technology would be able to perform these human functions appropriately. As this type of model evolves it could instead prove well-suited for first pass review (similar to TAR), with the goal of reducing costs and optimizing legal workflow.

2. Models like GPT-3 will need to be trained on specific document sets in order to be useful for a specific organization's investigation or case. This will require a cost-benefit analysis and comparison to tools already deployed, as it will likely require significant training to be useful in this scenario.

3. Sometimes the chatbot will still answer inquiries incorrectly. This could be detrimental when utilizing for document review, research, settlement evaluation, motion drafting, or contract drafting. This does not mean that advanced language models will never be appropriate in such situations. Decision makers need to weigh the risks and benefits for each use case, which will be easier to do as more studies and statistics become available.

4. Training data will inevitably become stale, which means that models like GPT-3 will need to be continuously trained and updated in order to generate quality responses.

5. Lawyers always have to account for their ethical obligations when dealing with emerging technologies. Client confidentiality, security and privacy are some considerations that surface with tech usage. Putting confidential client information into a language model like ChatGPT will waive privilege and can violate the attorney-client relationship. Any information included in a prompt will not be deleted and can be used for training purposes. Consider these factors before using for document review, contracting, language translation, and other use cases that involve confidential information. Client consent is also crucial when using any new technology and lawyers need to remain informed about the benefits and risks in order to provide competent representation.

While language models are an exciting area that creates new avenues for innovation, fears of this technology replacing human expertise are unfounded. There are too many risks and factors that still require legal expertise and human judgment. In fact, even the creators of such models warn that their output should not be used for anything critical, independent of human review and analysis.

Large Language Models could initially gain adoption for creating simple templates, contract management, administrative automation, and some document review, but its use for legal research or brief writing seems unlikely anytime soon. Tools like ChatGPT do not account for factors such as a judge's preferences, unique processes, or client goals. In addition, unless these types of AI models are trained in a secure way, there is also no guarantee that sensitive information will be kept confidential.

What should legal organizations do now to stay ahead of the curve? Proceed with caution. Monitor developments with ChatGPT and similar tools. Limit use cases until more is known. Create policies and trainings around this technology usage. Advise corporate clients about the benefits and risks of using tools like this for business purposes. And, above all, have external partners that understand the technical aspects of emerging technologies to turn to for consultative purposes.

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 New Era of Legal is Here: Are You Ready?

The sky is falling! AI is taking the legal industry by storm and lawyers will soon be extinct! This was a common refrain amongst legal professionals in New York last week at the 2023 Legalweek conference. The good news? This is absolutely not true. Although the conference kicked off with a keynote speaker known for his famous role in the renowned sci-fi show Star Trek, we are thankfully not living in a sci-fi universe – even if many lawyers fear that to be the case. The expert panelists at Legalweek assured industry professionals that even the newest technology like generative AI cannot be a substitute for the legal mind. Machines cannot replace a lawyer's analytical skills or human judgement; however what technology can do is help legal departments automate routine tasks in a more efficient manner and allow legal professionals to concentrate on higher level work.

The legal industry is in a state of disruption - and disruption can be scary. At Legalweek's annual state of the industry presentation, there were frequent reminders that digital is no longer a choice in 2023. Everyone in the legal community is in some stage of their digital transformation journey. The technology is available today and will continue to evolve, but throughout this journey it is the right combination of people, process, and technology that will be key to successful outcomes. While tech is important and will continue to open new opportunities for legal departments and law firms, it is only a tool, not the end game.

Embracing Change

Now is the time for the legal industry to begin to reassess how the law is practiced and create a coherent strategy around using AI to tackle challenges and increase efficiencies. That starts with top-down support and bottom-up buy-in throughout the enterprise. Having the right talent internally is important, but partnering with providers and consultants that can fill gaps and effectively implement the tech is the key to effective change.

Three major themes from Legalweek are worth considering as the industry navigates this new era.

#1: AI is a disruptive force in the legal space and lawyers need to prepare.

A new survey by LexisNexis demonstrated that 86 percent of lawyers were aware of generative AI and over half used or plan to use this tool for work purposes. Additionally, 84 percent of lawyers surveyed felt that generative AI would increase efficiency for their legal team. Even with all of these high stats, only 39 percent agreed that it will significantly transform the legal practice. This mirrors what happened at Legalweek, with ChatGPT unsurprisingly winning the MVP for most explored topic during the conference. While there was a lot of excitement and willingness to learn more, there was also hesitation and fear.

What is clear is that large language models like GPT-3 and bots like ChatGPT are here and evolving quickly. The time is not far off when providers will start integrating this tech into their existing tools and clients will regularly use these tools for business purposes. Lawyers need to be proactive

and keep tabs on developments and find ways to close the knowledge gap surrounding AI tools. Tech is not one size fits all. The right people need to vet the technology ensuring it benefits the organization as a whole. Working with various internal stakeholders to understand requirements can ensure the right technology is chosen for the task. Also important is understanding that technology does not always work on the first try. It is an iterative process that takes time to train both the system and end users.

While there was talk about potential use cases for generative AI – from automation to negotiation playbooks – the focus was really on the people and processes needed to get there. There has been a noticeable shift over the last decade with more lawyers embracing AI tools in several areas including eDiscovery, contract review, and compliance. The benefits are plentiful – cost optimization, improved outcomes, retention enhancement, and more. Similar benefits are likely to unfold with generative AI. This will require a deliberate process of evaluating impacts and opportunities by bringing in consultants who can help decide where AI tools may be beneficial and partnering with providers who can help navigate their use in areas such as eDiscovery collection.

#2: Commitment to change management is key to successful transformation.

The practice of change management is not new, but it can be difficult to implement effectively. At its core, change management is simply the approach an organization takes to managing change during times of transformation. A mix of new ideas, strategies, and oversight is necessary to manage change during a time of disruption. This should be a top priority for organizations navigating the era of generative AI, and the focus should be on who the right people are to drive change within an organization. Look for people that not only know the tech, but also how to implement it effectively on a broader level and for case-specific needs, educate internally, and demonstrate value to stakeholders.

With legal currently being a multi-generational profession, change management related to new tech adoption can be tough. Having lawyers that run the gamut in age is a hurdle. There are those that do not want to change their processes that have worked for years; young professionals that are curious about tech and starting to demand change; and those across various age groups that are dipping their toes in the water but still have hesitation. Legal as a whole is starting to embrace new ideas, but lawyers are busy and may not be willing to devote the time it takes to see true ROI from a tool. This is where hiring outside parties to navigate change and illustrate how dividends can pay off down the road is key. Explore third parties that can perform legal spend analysis and advise on budget planning to help obtain approval from stakeholders to increase legal tech spend.

#3: Regulatory compliance is a growing concern.

Another big piece of the puzzle is compliance. AI tools inevitably invoke privacy and data security concerns. In addition to privacy regulations around the globe, regulation of AI is starting to materialize. The rise of generative AI will most likely accelerate regulation calling for transparency and accountability, so lawyers need to partner with experts that can navigate these complicated waters and drive compliance as the adoption of these tools increases.

By now, every organization should have regulatory compliance and data security programs. If roles are not created internally and there is a lack of outside expertise to turn to with questions, this will become increasingly hard to manage. The use of new tech always brings risks that organizations must evaluate before investment. Beyond education on new privacy or AI laws and trending cyber-attack methods, it is crucial to have policies in place around how to comply with various regulations or respond to a breach. On top of this, lawyers have an ethical obligation to their clients to keep information confidential.

Conclusion

So, will machines replace lawyers? The answer is no. However, AI opens up a lot of opportunities for meaningful change. Right now the focus should be on tech education, partnering with the right people, and improving processes. The better technology the legal team has on hand, the better equipped they will be to provide meaningful value to the business. Legal is moving away from being the "department of no," to the department of innovative ideas.

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 Bankruptcy Courts Shape Crypto Regulation?

Last year's cryptocurrency market crash a/k/a "the crypto winter" did not cause trembles in the U.S. economy, but it caused enormous losses to its investors. The near collapse of this decentralized currency market resulted in bankruptcy filings by several cryptocurrency exchanges. Creditors have been waiting with bated breath to see how the courts will decide key questions such as how will the tussle between the US courts and the Bahamian authorities play out; what assets are allocated to which entity; what will recoveries look like for creditors; and would criminal restitution against founders and directors be part of the US bankruptcy? How judges rule on these issues will certainly provide crucial insolvency guidance for the owners, investors, and regulators of crypto assets.

Given recent governmental actions in this sector, it appears that 2023 will be the year of crypto regulation. As the issuer of the dominant global fiat currency, the U.S. would be the most likely venue for devising a global crypto regulatory framework. Cryptocurrency currently lacks a centralized framework of trust aka "intermediaries" and its "trust" relies solely on the verification methodology with the blockchain for those transactions. The absence of regulation has certainly made it possible for the rapid growth of exchanges but unfortunately for investors has also allowed undetected fraud. The U.S. system of a centralized finance is credited with protecting consumers and investors, ensuring financial institution stability, curbing illicit finance, and maintaining economic competitiveness. Not surprisingly, the U.S. bankruptcy courts are the first official tribunal confronted with issues of first impression with respect to debtor and creditor rights. The decisions made by bankruptcy judges in these initial cryptocurrency cases will guide the course of regulatory framework and compliance protocols for this new asset class. Current and future crypto investors need to monitor these court decisions along with regulatory activity that will likely occur this year.

The Regulation of Money

The U.S. dollar has been the dominant global currency for decades. Money is regulated through the U.S. central bank – The Federal Reserve aka the "Fed". This oversight body

regulates U.S. currency and essentially controls the supply of money. This allows banks to operate for consumers within a centralized finance system with multiple layers of monitoring and compliance. While a structured regulatory approach creates an atmosphere of trust, it is extremely expensive to maintain. Processing funds and confirming balances on this system requires extensive staffing for a majority of critical functions, monitoring tools, investigations, and much more.

The U.S. has continued to refine its monetary policies throughout the past century. The Fed was in fact created as a response to the Panic of 1907 when a cooper mining trust collapsed along with all its investors' funds. Regulatory policy historically arrives soon after major financial disruptions like the Great Depression, the 1987 Stock Market Plunge, September 11th, the Great Recession, and the Covid-19 Pandemic. More recent policy examples of those are the Sarbanes-Oxley Act of 2002 and Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010. Sarbanes-Oxley mandated several reforms to enhance corporate responsibility, enhance financial disclosures, and combat corporate and accounting fraud. In 2010, Congress passed the Dodd-Frank Act in response to the crippling financial crisis of the Great Recession in 2008. This law aims to reshape the U.S. regulatory system in areas such as consumer protection, trading restrictions, credit ratings, regulation of financial products, corporate governance, and disclosure and transparency.

After the Great Recession, the U.S. made it a priority to institute regulatory controls that would "contain the contagion" in the event of future collapse of any aspect of the financial system. This protection is evidenced by the limited effect that the crypto market crash had on the overall economy. Despite the containment within the crypto sector, the crypto winter hurt hundreds of thousands of investors and caused billions of dollars in losses. This decline in cryptocurrency values has prompted several bankruptcy filings which position bankruptcy judges at the forefront of providing guidance to the crypto industry, its investors, and federal regulators.

Takeaways

The crypto crash can serve as a guide on how to protect investors in this new asset class. What are the lessons to be learned? First, the rapid decline of the crypto market in such a short period of time points to the shortcomings of a decentralized financial system. Because of the lack of structural trust, many investors suffered great losses that could have been avoided or at least limited if there was some federal oversight.

Second, because of the declining value of the crypto market, investors are signaling that they want more transparency and faith in the stability of currency. Preliminary investigations have revealed that this was not an issue concerning any failure of the underlying blockchain technology, but rather the actions of the exchange principals. The crypto winter was a direct result of the absence of checks and balances on this decentralized financial system. Supporting a system of compliance to ensure things are above board and comply with future regulations will be necessary to instill a baseline of trust in this sector.

Regulatory Predictions

Regulation often comes on the heels of a crisis. With a new session of Congress just beginning, crypto regulation will definitely be a hot topic on the table. Lawmakers are becoming more educated about digital assets and any law on this topic will need bipartisan support. What is likely to happen is that crypto industry will be subject to newly created regulations and well and lawsuits for violations of exciting securities laws. These rules will most likely come from several federal agencies: The Securities and Exchange Commission (SEC), The Office of the Comptroller of the Currency, The Federal Deposit and Insurance Corporation (FDIC), and the Federal Reserve. In fact, these agencies just issued a joint letter voicing their concerns about all crypto assets. After the fall of the FTX exchange, the federal government and Congress turned its focus on this sector. The decisions from the bankruptcy courts will provide guidance on many legal aspects of these assets when the exchange is insolvent. The decisions made by these courts could expedite the regulatory framework required to support a stable cryptocurrency market.

Below are three predictions on what may happen soon:

Any regulation that is enacted will have some aspects of our existing financial regulations. Decentralized finance systems are proven fairly unstable when tested so there must be some protections built into its structure. The case for stronger oversight is more compelling as we've seen these exchanges seek bankruptcy protection but it is unclear how they will emerge and make distributions to creditors.

- The bankruptcy courts will issue key decisions on the interplay between various courts asserting jurisdiction, what is property of the bankruptcy estate and which entity and whether these companies will ultimately liquidate or survive. For example, in the Celsius case, the judge relied on the terms of use disclosure to find that the users no longer possessed ownership rights over the digital assets. This means they will be treated just like any other unsecured creditor.
- Estimates of creditor recoveries are not known at this time. Bankruptcy courts will need to determine the order of creditor payments, which will set precedent for future matters.

Additionally, here is a recap of important activity in the crypto regulatory space:

- The agriculture committees in both the Senate and House have been brainstorming bills that would provide the Commodity Futures Trading Commission (CFTC) crypto regulatory powers. In a February conference, the CFTC stated that it would be well-suited to regulate cryptocurrency that is not viewed as a security to ensure these assets are monitored effectively. Some have expressed concern that strict rules and CFTC oversight would hinder the decentralized finance model.
- The White House recently released a statement outlining a roadmap to mitigate crypto risks. This included a call to action for Congress to expand regulatory powers to combat misuse of customer assets. Also, to strengthen transparency and disclosure requirements for crypto companies.
- The SEC has been cracking down on crypto-related enforcement. In February, the SEC filed charges against Kraken for failure to register the offer and sale of their crypto asset "staking as a service" program. Kraken

instantly acted to settle this matter by paying $30 million and stopping the program.

- The SEC also notified the crypto firm Paxos that it will commence an action against them for issuing of the Binance-branded BUSD stablecoin that the agency views as an unregistered security because it was pegged to the U.S. dollar. The SEC points to the company's lack of appropriate financial disclosures and notice to investors concerning the risk associated with stablecoins. Paxos has expressed intent to litigate the issue of whether BUSD should be considered a security, as it disagrees with the SEC's characterization. The New York Department of Financial Services has also ordered Paxos to stop issuing BUSD in February 2023.
- On January 3, 2023, the Federal Reserve System, the Federal Deposit and Insurance Corporation, and the Office of the Comptroller of the Currency issued a joint statement on crypto assets to banking organizations. These regulators warned U.S. banks that there is increased fraud potential, uncontrolled risks, and volatility with crypto that could cause immense harm if allowed to seep into the banking system.
- Money-center banks are backing away from crypto companies as talk of regulation crack-down threatens their access to traditional banking products. The inability to use bank accounts in the US will severely hamper their ability to transfer fiat currency.

Crypto is a new frontier that needs some oversight to survive. Once the bankruptcy cases are resolved, there will be guidance on some important issues and how to reorganize or liquidate these digital asset companies. In the meantime, keep track of enforcement trends and how agencies like the SEC, FDIC, OCC and the Federal Reserve System. Also, whether any traction is made by Congress establish new laws – especially after the White House spoke recently on this topic. It appears that 2023 will be the year of crypto regulation.

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.

Deirdre O'Connor is a managing director in Epiq's corporate restructuring business in New York. With over 25 years of restructuring experience in law, corporate finance, government and technology enabled solutions, Ms. O'Connor drives enterprise-wide initiatives to strengthen and expand Epiq's corporate client relationships.

Three Pillars of a Modern Legal Team

How are modern legal teams approaching eDiscovery and what industry themes are surfacing? All eDiscovery professionals should be pondering these questions as more organizations embark on transformation journeys. Innovation has increased and there is a focus on how to be strategic, make purposeful investments, and offer growth opportunities to the legal team. How is this all possible? While legal tech is a driving force in carrying out meaningful change, getting the right people with the right skillsets in the right places to close the gaps is what seals the deal.

Common themes that keep eDiscovery professionals across practice areas up at night include lack of technology and buy-in from upper management, uncooperative attitudes that limit capabilities, and the desire to maximize human potential. There is also increased focus on team growth, retention, employee well-being, and cultivating company culture. Making strides in these areas can help modernize legal teams and maintain a competitive edge.

Three main areas to focus on when modernizing legal teams and eDiscovery processes are collaboration, automation, and standardization. All of these components are intertwined and will drive change when harmonized and prioritized.

#1: Collaboration

Everyone talks about the importance of collaboration, but do they really practice what they preach? Innovation unfolds by seeking out collaboration opportunities not just within respective teams, but with everyone involved in a matter. There are gaps that need to close between legal departments, outside counsel, and alternative legal service providers. Collaboration can also be beneficial outside the immediate project team by connecting deeper with third-party experts and other industry contacts. These opportunities often take a backseat to technology, when in reality the exchange of ideas and planning meetings are crucial to choosing optimal tools. When there is a disconnect between preservation and presentation, inefficiencies emerge due to lack of communication or being unaware of emerging technologies that will solve recurring problems. There needs to be a more concerted effort to bring everyone to the table via planning meetings, status calls, and new idea presentations.

Oftentimes the parties involved in a case are siloed and the more that regular communication occurs, the more the walls will break down.

Consider these options:

- Invest in solid collaboration tools that provide one location to access case updates, communicate, integrate apps, and reuse prior intel.
- Have that initial meeting with the internal and external players at the outset of a case to align expectations.
- Employ a project manager to add value to the process.
- Check in with IT to see where internal security gaps exist so the team can proactively combat issues, continue to protect sensitive data, and maintain attorney client privilege.
- Perform legal spend analysis to help be more strategic about what should fall on outside counsel and what can be outsourced to a provider. For example, certain matters requiring specialized expertise or that are time/budget constrained may be better suited for a partner with flexible talent options versus outside counsel.
- Attend industry events to see what is working well for colleagues and competitors.

These are just a few ways to work on collaboration where the payoff manifests in smoother project management and increased efficiencies.

#2: Automation

While automation is not a new concept, there is so much more innovation potential when legal teams focus on what really should be automated and the tools at their disposal. Being strategic with automation can be a game changer. Automating in the right places also provides the opportunity for lawyers to elevate their talent as they will have more time to shift their attention to strategy, preparation, consultation, and complex issues that drive higher-value work for clients. This also frees up time to focus more on collaboration opportunities and invest in professional development, which more people are prioritizing.

As always with investing in automation, thorough vetting is critical and establishing longstanding relationships with trusted outside partner makes this process simpler. Any internal staff or external partners training tools to automate will need to have the right skillsets and knowledge to ensure the tech operates as desired. While eDiscovery projects are not one-size-fits-all, there is a lot of opportunity to automate where workflows repeat.

#3: Standardization

Standardization and automation are greatly intertwined. Teams cannot automate effectively without solid standardized processes in place. There is widespread desire in the legal industry to overall improve standardization efforts by exploring areas with untapped potential to create more uniform processes. This is crucial with high volume workloads, as there is just too much data to work through manually. While this seems like a simple task, it can be hard to know where to begin when there are so many unique factors in a case and divergences in how practitioners or external partners work. Start small with what is within reach and work up to standardizing across the different eDiscovery phases. Some examples include standardizing collection procedures, data handling via information governance policies, and preferred vendor usage.

Planning for the Future

To collaborate, automate, and standardize more effectively, there needs to be people on the legal team with the right skillsets. How to determine what is right? Remember this is subjective and will vary between organizations and case needs. Evaluate what can be repeated across projects and what is unique. The goal is to think critically and make informed recommendations, integrate emerging technologies, change and improve process, and drive adoption from the top down. This is possible with the right internal staff and external partners that work together as one unit.

Sometimes an eDiscovery managed services arrangement will be the answer to help manage legal matters with confidence. Using one provider that wears several hats can be valuable to improve legal tech education, find tools that every member of the eDiscovery team can benefit from, and improve collaboration. Besides having shared vision with an external partner – there needs to be internal stakeholders at law firms and corporations that collaborate effectively, the willingness to cooperate with adversaries, and continuous education.

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 Competition Regulation is Changing – How Can Organizations Prepare?

Five years from now, the global competition landscape will look completely different. Accelerated changes are materializing all over the world. There has been a distinct shift in the scope and breadth of investigations by global competition regulators as more become tech savvy. Tactics are changing and the focus is on compliance and getting ahead of issues as aggressive enforcement ensues. Given the increasingly international component of corporate transactions, it is crucial to keep apprised of competition reforms that occur around the globe. Canada has followed these trends by amending the Canada Competition Act. Some changes became effective last year and others are scheduled to kick in this June. Additional reform is currently being considered as well.

Organizations doing business in Canada or that are part of an international deal need to take note of how these changes are kicking off enforcement trends in Canada.

The Updates

In 2022 the Canadian Minister of Innovation, Science, and Industry launched a comprehensive review of the Competition Act. This was supplemented by a series of amendments announced in the 2022 federal budget that were largely technical in nature, but which provided an indication of the movement towards modernizing the Canadian competition regime. The expansive antitrust agenda launched by the Biden administration has influenced this activity in Canada, as merger filings and reviews are surging. Global regulators are seeing the value in cross-border collaboration to hone in on the real issues and effectuate meaningful change.

The Bureau's evidence gathering powers under Section 11 have expanded, which means that there is higher potential for large amount of data requests during an investigation. Other significant updates apply to mergers and litigation.

Merger review: There are new non-price factors for the Competition Bureau to account for when investigating a potential merger. These factors are network effects within the market; potential for the merger to entrench the market position of the top competitors; and how the merger would influence price, quality, choice, and consumer privacy. There

is also a new "anti-avoidance provision" that will ensure all required transactions are subject to the law's pre-merger notification provisions. Some parties were circumventing this in the past by intentionally structuring deals in a way that would avoid notification and pre-closing approval.

Litigation: Three amendments are expected to increase the scope of private competition litigation and class actions – a new wage fixing/no-poaching agreement criminal offense; labeling drip pricing as a deceptive marketing practice; and expanded rights for abuse of dominance, including allotment for a private right of action and increased financial penalties.

The no-poach provision becomes effective this summer, so now is the time to review employment agreements and HR practices to ensure they are up to par. The amendments to the abuse of dominance provisions expands the types of conduct captured to include practices that "have an adverse effect on competition" or are "a selective or discriminatory response to an actual or potential competitor."

Additionally, on March 15 the Bureau responded to the government's request for public consultation on further reform to Canada's competition landscape. The Bureau's recommendations are lengthy and would essentially rewrite the current law. The changes would apply to merger review, unilateral conduct, competitor collaborations, administration and enforcement processes, and deceptive marketing. Some key changes proposed are increasing evidentiary burdens and

restricting timelines during merger review, criminalizing buy-side agreements, and administrative penalties for competitor collaborations.

How to Prepare

With the current amendments and more likely on the horizon as Canada's competition reform ensues, organizations need to prepare. Expect more focus on issues outside competition such as ESG concerns, as well as broader data requests.

Here are three lines of defense to implement to help remain compliant and ahead of the curve:

1. Prepare for the Increased Litigious Nature of the Bureau: Understand that Canadian competition regulators are operating under the mindset of: "what is the risk of not taking action?" The Bureau is building investigation and litigation capacity so that it is able to bring timely and evidence-based enforcement actions, focused on both traditional and digital marketplaces. Predicted trends are increased willingness to advance novel or aggressive theories of competitive harm, while being less accepting of remedies or modifications that parties suggest.

   Parties need to be more cautious during negotiations. Consider the parameters of how far a deal can go and when the Bureau may intervene. Also keep in mind that regulators are now considering non-price factors when deciding whether to investigate.

2. Managing Increased Data Volumes: Global collaboration, expanded issue scopes, and aggressive enforcement against anti-competitive behavior inevitably results in more data being subject to an investigation. Organizations need to have a firm grasp on where data resides and how to follow communication trains in the hybrid environment. Focusing on compliance and being proactive will help spot issues earlier and better manage data overall.

3. Prepare for the Rise in Corporate Investigations: The Bureau recently launched a compliance portal to support organizations in building credible and effective compliance programs. The portal includes guidance around risk-based compliance assessments, compliance training and communication, monitoring, and ongoing compliance evaluation. Having a solid program will help tremendously if a competition investigation ensues. This can aid in quickly demonstrating diligence and persuade the Bureau to pursue a civil track offense rather than a criminal track offense; lower monetary penalties; and provide support for granting a leniency application.

Given the scope of amendments and what is on the horizon for the Canada Competition Act, organizations should be completing compliance program assessments now to make things more smoothly when enforcement efforts ramp up. Adopting a risk-based approach and underlining compliance as a key component of a company's corporate culture helps it to maintain a good reputation, internally and externally, thus avoiding infringements by educating employees and mitigating risk factors before they occur. Training and open lines of communication are key enablers of this goal.

To create these defenses, organizations need to implement a tech-enabled strategy. This requires a probe into current processes and partnerships to identify areas that are lacking efficiency or missing potential issues. Start early and leverage AI to understand company data and risk factors. Implementing eDiscovery processes and tools can help with this feat and speed up the process. It is critical to partner with a provider who has bespoke and defensible solutions for collecting and analyzing different data sources. This will help keep pace in Canada and also before other global regulators that are ramping up competition enforcement efforts and changing approaches.

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.

Using Metrics to Tell a Story with Data

"Data is the new gold." This adage is popping up across industries as more organizations recognize the value that lives in business data. When properly harnessing information and tracking metrics that actually matter, true value will emerge. Decisionmakers will be able to visualize where gaps exist and how to close them, where there are collaboration opportunities across departments, and where there is inefficient spending. This is gold.

The legal department is an optimal place to gather metrics that can help make better business decisions not only for legal – but across the entire enterprise. Hyperion Research's 2022 benchmarking survey of Legal Operations professionals found that 63 percent of Corporate Legal Departments have formal metrics and analytics programs, but only 9 percent have metrics that are well-defined, curated, and have audience-specific dashboards. Without the latter, legal teams miss business intelligence and meaningful insights.

Organizations seeking to transform their metrics and analytics programs should ask these two questions: what data should the legal department track and what tools can help?

Question #1: What Data Should Legal Teams Track?

The answer to this question is a lawyer's favorite: it depends. Now is the time for organizations to be creative and think through what KPIs to measure and metrics to collect in order to get actionable legal and business intelligence. This can come from many different areas, but cost savings and efficiency will always be at the forefront. Instead of merely focusing on where to cut costs, working backwards through a strategic lens to uncover savings is key. Maybe there is an outdated litigation workflow that has been overlooked for years. Or the legal department is failing to tie what they are tracking into overall business goals, which can be difficult depending on what leadership is prioritizing.

Here are three areas to consider exploring further:

- Business transformation: In a hybrid working environment, many organizations are realigning their operational strategies. There is an opportunity to scale productivity and maximize resources by reimagining traditional employee role, downsizing real estate, and changing outsourcing priorities. This presents opportunity for not only legal, but the entire enterprise. How many employees are working remotely and how often? How often are meetings held in the office versus remotely? What departments need physical space and how often? Are legal documents and mail that could be routed digitally still stored onsite and how much space and resources does this take up each month? These are just a few simple data points that could shine light on the need to reimagine office services. This may include hospitality, reception, conference room management, digital mailrooms, print, and information management services.
- Staffing and retention: More organizations are prioritizing offering employees better benefits and resources to improve retention, work-life balance, and mental well-being. Legal can coordinate with HR to track not only headcount trends – but also whether retention improved after certain initiatives or benefits rolled out, DEI efforts, and more. Being able to illustrate this to leadership will help exhibit compliance with company culture and objectives. It can also shine light on recruiting needs, start dialogue about redefining workflows, and make it apparent where flexible legal talent could improve efficiency or support department in times of attrition.

- Redesigning eDiscovery workflows: Litigation is often the largest component of legal budgets, with a big chunk of investment going towards eDiscovery tasks. Advancing an eDiscovery health check with an expert consultant can help transition a fragmented program to a long-term eDiscovery strategy. One path is creating a roadmap after targeting gaps and inefficient processes so teams can implement foundational changes. Determining appropriate metrics to measure should be a part of this roadmap in order to bring true value and cost reduction to the department. Examples include breaking out legal spend for each phase of eDiscovery and comparing settlement value; case performance broken out by jurisdiction or issue; and cost analysis after utilizing new legal technology. Being able to get more granular will help demonstrate the true benefits from a new solution or process, while also shining light on inefficiencies so teams can continue to advance change.

These are just a few examples of some unique ways to curate and define metrics. Additional ways legal can partner with other areas of the enterprise include looking at how many deals legal helped the sales team close; reduced litigation exposure from removing ineffective contract clauses; and savings incurred after changing the way work is divided between in-house staff, outside counsel, and provider partners. Remember that what data holds meaningful insights will differ between organizations. It will also change as new projects or goals materialize, company culture evolves, and benchmarking opportunities unfold.

Question #2: What Tools Can Help Track Data in a Meaningful Way?

It can be a challenge to determine what and how to measure in the face of an increasing need to integrate data from various legal technology sources. The first step is bringing the right people to the table to align expectations. Establishing a committee with members from various levels at the organization that meet at least yearly can be beneficial. Some participants to consider including are legal, HR, C-suite, departmental managers, risk, and cyber. This will provide a space to discuss company objectives, facilitate cross-departmental cooperation, and determine what story legal's data needs to be telling. Knowing how the organization measures value increases legal's visibility which results in improved data optimization and tech scaling capabilities.

Look for tools that generate metrics tracking KPIs and tie KPIs to business objectives. This makes it easier to demonstrate wins and progress to upper management. To help with this feat, consider bringing in an external provider that offers solutions with customizable dashboards, data libraries to benchmark against, and ongoing support for analyzing and presenting data. Look for a partner offering a single platform that can pull data from several operational sources (such as e-billing systems or matter management software), and then present the data via intuitive dashboards that help tell the right story.

Important features to look for in a platform include simple deployment, report generation, single sign-on capabilities, ways to compare metrics and visualize benchmarking, KPI catalogues, data classification, tool integration, access to industry data, and enhanced security features.

Delving into these two questions will enable legal to be a better data storyteller and demonstrate value across the enterprise.

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.

Spring 2023 Data Privacy Updates

How can organizations remain privacy-compliant in a world where differing laws keep emerging? This is a continuous struggle for many as new developments materialize around the globe. From amended laws to entirely new frameworks and aggressive enforcement, more U.S. states and countries abroad are drastically altering their data privacy landscapes.

There is no indication this will slow down anytime soon, so understanding relevant laws is crucial to maintain proper compliance. When conflicting responsibilities surface, it can be difficult to manage. Having a team dedicated to compliance and tapping into outside resources to help manage these obligations is becoming increasingly necessary.

Keeping tabs on the changes is half the battle, so here are a few privacy happenings so far this year to understand and monitor.

U.S. Update

The data privacy landscape continues to grow in the U.S. with Iowa being the sixth state to pass comprehensive legislation in March. The Iowa Consumer Data Protection Act will become effective Jan. 1, 2025. Iowa protections align most closely to Utah's privacy law, placing it in the more business-friendly category. The law lacks the following: a monetary threshold to apply, private right of action, a data minimization requirement, and data protection assessment mandate. Allotted penalties are $7,500 for each violation, which means liability can be high depending on the nature of the breach.

Three other state legislatures also recently passed laws and are awaiting governor approval: Indiana, Montana, and Tennessee.

- If approved, the Indiana law will become effective Jan. 1, 2026. It aligns more with Virginia's privacy protection, which is middle of the road between being consumer or business friendly. Distinguishing features include lack of a private right of action; exemption for facial recognition collection on riverboats when there is prior approval from the Indiana gaming commission; and, a requirement that organizations perform impact assessments for some processing activities, such as those involving sensitive data. Indiana also allows penalties up to $7,500 for each violation.

- If approved, the Montana law will become effective Oct. 1, 2024. It tracks the Connecticut privacy law closely, which also takes a more neutral approach. The Montana law has stricter privacy requirements for children, requires data protection assessments, lacks a private right of action, and grants universal opt-out options to consumers.
- If approved, the Tennessee law will become effective July 1, 2025. This law leans a bit more business friendly than the bills proposed in Indiana and Montana. While it has typical requirements such as data protection assessment requirements and the right to cure, it is the first state to mention the U.S. National Institute of Standards and Technology (NIST) privacy framework. To remain compliant under Tennessee law, covered organizations may need to adopt and follow NIST standards.

Several other states have introduced – or will introduce – bills to get their own privacy laws on the books. Analysts have pondered whether states would start to follow a trend modeled off one style of law, but as more pass, it is becoming

apparent that this is not happening. Instead, the patchwork of privacy legislation is becoming messier. Even when modeling off another state law, each has distinguishing features or have integrated features from several laws.

There is still debate over passing the American Data Privacy and Protection Act at the federal level, so until then, state directives will continue to control compliance.

Global Update

Two countries that have made significant strides in 2023 to enhance their data privacy landscapes include Brazil and Australia.

Brazil

Brazil's General Data Protection Law (referred to as the "LGPD") went into effect in August 2020, but the criteria for issuing sanctions was not released until earlier this year. The LGPD applies when an organization processes personal data that is in Brazil or collected in Brazil. The LGPD has expanded consumer rights, including the ability to access information about anyone who has given their personal data and the right to request whether an organization stores certain data.

The Brazilian Data Protection Authority has received a large amount of violation complaints and data breach notices, finding the presence of inadequate safeguards in eight matters as of March 2023. Enforcement is expected to pick up now that there is clarity around sanctions. Warnings, partial or total bans on data processing activities in Brazil, and financial penalties are available. Fines can be up to two percent of an organization's revenue with a cap of 50 million Brazilian reals (which is just below one million USD) for each breach under the law.

The Brazilian Data Protection Authority has expressed it will start with warnings and small fines before issuing severe penalties. Regulators will also take various factors into fine calculation, including how serious the violation was, what type of data is at issue, whether the party made any good faith efforts to appropriately protect the data, and how quickly a party corrects infringements. This illustrates that the regulators understand compliance will take time as the landscape evolves, they will work with organizations to get their compliance programs up to par, and more leniencies will be afforded when there is evidence of good faith efforts to protect personal data.

Australia

Over the last five years, major reform to the Australian Privacy Act of 1988 has been in the works. Last December, amendments were quickly approved after Australia experienced a wave of harmful data breaches. Increased fines are now available and can be the greater of $50 million AUD (which is about $33 USD), three times the value of the benefit derived from a breach, or 30 percent of adjusted turnover. The Office of the Australian Information Commissioner also now has expanded enforcement powers to tackle breaches more expediently and efficiently.

In February 2023, more progress was made after the Attorney General's office completed a long-awaited review of the law and offered 116 new proposals. Overall, the goal is to keep the law intact but greatly expand consumer protections to be closer to the GDPR. Proposals include adding a right to be forgotten, availability of private actions for certain breaches, more regulation over targeted advertising, public transparency requirements, strengthening the definition of personal information, and security enhancements for international data transfers.

The public comment period on these proposals closed at the end of March, so more movement on this front is expected at some point this year.

Other Significant Data Privacy Developments

Other countries across the globe continue to make privacy enhancements each year, so it is crucial to know which global laws apply and watch for any changes. In addition to Brazil and Australia, here are two other global events to note:

The Italian Data Protection Authority banned the use of the generative AI tool ChatGPT. It is currently investigating whether this tool violates the GDPR for failing to notify individuals that it collects and processes personal data for training purposes. What comes out of this investigation could influence other regulators' stances on this popular tool.

A pending privacy bill in India has received 40 proposed amendments, which will likely present further delay to passing this legislation. Major concerns included lack of protection over child data, broadly written exemptions, and insufficient powers granted to the proposed regulatory body.

Conclusion

If an organization does not have personnel or provider partners to help with privacy compliance, now is the time to change that. The above is only a snapshot of the progress made on a global scale. New legal obligations will continue to emerge, and it is safe to say that many organizations will deal with conflicting directives. It is pertinent to know which laws apply, have compliance programs that account for differing processes depending on data being handled, document compliance measures to remain defensible, and cooperate with regulators as they also navigate these changes.

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.

Is it Time for a Discovery Health Check?

The world of eDiscovery is in a constant state of change. Modern data sources expand the pool of relevant information and may warrant special collection techniques. Court decisions and rules create new precedent and can alter deadlines. Emerging technologies warrant new ways to manage eDiscovery workflows. Client demands may call for unique processes or outside expertise. Whatever the obstacles may be, many legal departments have a fragmented eDiscovery program. Developing a long-term strategy can close operational gaps and uncover cost-savings opportunities. This is where performing a discovery health check is transformative. Organizations can make foundational and sustainable changes by implementing documented workflows, using advanced techniques, and developing trusted partnerships.

Industry Challenges

In the 2023 State of the Industry Report, eDiscovery Today and EDRM surveyed a mix of law firms, corporate counsel, service providers, consultants, government entities, and other legal professionals. When asked what eDiscovery challenge not enough people in the industry are talking about, the top response at 23.4 percent was lack of eDiscovery competence within the legal profession. Other top challenges included in-place indexing and the move to the left of the EDRM Model, discovery of collaboration app data, increased compliance activities resulting from data privacy trends, and increased cybersecurity to support more dispersed workforce.

Implementing an operational and financial assessment of a legal department's discovery processes and procedures can bolster eDiscovery competence and help teams tackle other obstacles with confidence.

Performing the Assessment

Just like going in for a yearly physical at the doctor's office, legal departments should be periodically checking on the health of their discovery program. In a dynamic industry, it is crucial to assess how programs are faring comparative to market conditions. This calls for consultants who can leverage field expertise and proprietary data models to identify specific

action items, timelines, cost-saving strategies, and budget expectations. The result? Legal departments will be able to optimize in-house time and resources, reduce eDiscovery spend, and create long-term sustainable strategies to continue building upon for years to come.

Such an evaluation will require upfront investment and time, kicking off with strategy and planning to align expectations. A good place to start is connecting consultants with the legal team and other key stakeholders within the organization. Expect staff interviews, outside partner interviews, AI-driven billing analysis, and metrics analysis during the assessment. This will require collaboration between the organization and consultant in order to develop appropriate and meaningful insights.

Available Benefits

Here are five examples of what legal teams can gain from diving deep into their discovery program:

1. A consultant that can provide an action memo with recommendations at the end of the health check and a roadmap to guide future decisions is valuable. Legal can review and factor in their own perspective to account for costs, budgeting constraints, ROI, case priorities, and other variables. This will also illuminate pain points so the legal department can strategize what issues to tackle first.

Having a roadmap leads to long-term benefits including better control over eDiscovery processes, enhanced cost predictability, risk mitigation, enhanced defensibility, informed decision-making driven by legal business intelligence, and much more.

2. Legal's goals will align better with the company's business goals and requirements, which helps manage internal buy-in for investments by illustrating long-term ROI. This strengthens relationships and develops trust with internal stakeholders.

3. The opportunity to re-evaluate current technologies comes to the forefront and it may become apparent that an alternative technology is better suited for a specific process. This can shine light on functions that should stay in-house or be outsourced. It also provides an opportunity to update and enforce outside counsel guidelines so the right tasks are getting in the right hands. All of this allows legal teams to work as efficiently and cost-effective as possible.

4. Consultants can advise on the appropriate metrics to measure in order to bring true value and cost reduction to the business. Getting more granular is key to demonstrate the need for change, such as looking at cost expenditures before and after utilizing new legal technology and benchmarking against industry data. This can also uncover opportunities to work differently, such as reusing work product or developing portable AI models.

5. Having a better view into the health of the legal department's discovery program develops and strengthens partnerships with consultants, outside counsel, and other provider partners. This fosters better collaboration and a more seamless way to tap into outside resources when necessary.

The goals set for an assessment will look different for everyone, which is why customization and flexibility are key. The underlying focus will be to receive a holistic view of the program from both an operational and financial standpoint. This information allows teams to bring business concepts to the legal department, set a range of goals with timelines, optimize human and technology resourcing strategies, determine ways to use discovery workflows outside of litigation, and reduce eDiscovery spend.

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.

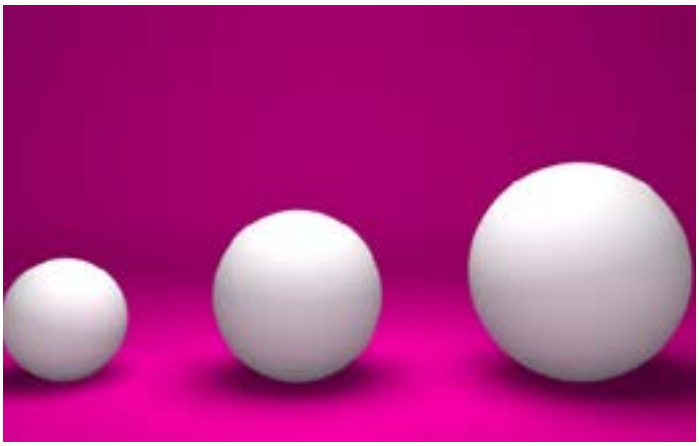
Welcome to the Third Generation of ALSPs: The Future of Legal Service Delivery

A new breed of Alternative Legal Service Providers (ALSPs) is entering the scene. These providers are considered "third generation" because they take the most innovative approach to legal service delivery. On top of having the right people, processes, and technology to meet a variety of needs – third generation ALSPs can also generate legal business intelligence. This is truly transformative, as it provides actionable insights for not only the legal team, but also the entire business. When ALSPs first emerged two decades ago, legal demands were changing as technologies advanced and data became more difficult to manage. Having outside support to navigate digital changes quickly proved beneficial from both cost and efficiency standpoints. Competencies have continued to evolve alongside legal tech sophistication. Expanded use cases today now include managed services, legal tech consulting, compliance, flexible staffing, contract analysis, legal spend management, business advising, data breach response, and class action administration.

Over the years, the ALSP market has gone through distinct stages of growth. Depending on what services are offered, providers can be categorized as first, second, or third generation. Understanding the distinctions will help legal teams make informed decisions on which type of partner can meet their needs and facilitate meaningful transformation.

First Generation: People

This represents providers that can help close process gaps quickly at a lower cost by reorganizing the "people" element of the legal team. They can provide people often, quickly, and at scale. These ALSPs emerged in the mid-2000s to offer legal process outsourcing models and assist with high-volume tasks, including but not limited to document review, litigation support, contract management, and flexible resourcing models to legal staffing. By having the right people with the right skillsets, they can help legal teams close gaps in these areas and work more efficiently. Oftentimes only offshore staffing and data storage options were utilized. However, as the market evolved "on-shoring" options at closer low-cost hubs also became available.



Second Generation: Technology

As ALSPs have matured, so have their capabilities and expertise. The evolution to the second-generation of ALSPs occurred around 2015, bringing technology offerings. At first, they were limited to automating inefficient legal processes, making legal support available to other departments on a self-service basis without the need for intervention by the in-house legal team, and gathering data about legal department operations to present it in a more easily consumable format. Over time, capabilities and expertise have matured. While still able to help with routine review and management tasks, second generation ALPSs offer advanced technologies and knowledge on a variety of disciplines. This includes AI-powered solutions for litigation and contract analysis, compliance services, automation capabilities, and more.

Third Generation: Legal Business Intelligence

An innovative type of ALSP is emerging that is focused on innovation more than ever before. These providers help legal make moves that will benefit the entire business. They leverage process optimization principles to make improvements to legal business performance that really move the needle. They can offer the above and consult on areas such as legal technology, metrics, project management, and legal

operations. A third generation ALSP will have a data science team that can pull data from a variety of sources into a single repository. This allows for the creation of true legal business intelligence that the legal team can use to make decisions about strategy, partnerships, and future investments. Making all legal data accessible and actionable allows GCs, and the firms that advise them, to see where they need to direct or optimize legal work and resources.

To summarize, a third-generation provider combines the following components:

- People Business Model Innovation: This involves having the right people to fill gaps in legal workflows, such as offering flexible talent and secondments. This can be either physical staff or virtual workers, depending on the client's needs. Third generation providers have AI-enabled virtual workers on staff that can meet demands quickly and efficiently from anywhere in the world. More providers are also offering consulting services with the rise in legal tech solutions and obstacles to data management.

- Technology-based Innovation: This focuses on having the right technology to enable digital transformation, thus presenting legal teams with ways to work more efficiently and consistently. Understanding that this is not a one-size-fits all approach and will highly depend on a client's fluctuating needs is crucial. Examples of technology these ALSPs will often have at their disposal include modern cloud-based platforms, analytics, and new AI models.

- Modern Process Innovation: This layer of competence is what sets third generation ALSPs apart as they operate through a future-thinking lens. Modern process innovation is about being able to not only make all legal data accessible but to then synthesize it into legal business intelligence over one secure platform. Accessibility includes the creation of modern dashboards—based on KPIs that are important to each individual business—that are consumable by the legal team and business leaders. With the increasing pressure to serve the needs of the business and reduce costs, having a partner that empowers legal teams to re-envision the delivery of legal services is vital to long-term success.

- Proactive Metrics: Third generation ALSPs will help legal teams track metrics that matter, understanding that this is not a "one-size-fits-all" concept. Integration and visibility via an intuitive dashboard with access to KPI catalogues is vital. Being able to customize metrics and track data points that can materialize as valuable business intelligence will truly transform legal's role within the enterprise. The goal for ALSPs possessing such capabilities is finding ways for legal teams to use their data to get ahead of issues proactively versus responding reactively after an issue already surfaces. Take contracts as an example. Having a more granular view into what obligations exist in an organization's contracts or cost and valuation metrics will help legal get ahead of issues that could surface from regulatory constraints, renewals, budgeting concerns, or other events.

Sound familiar? All of the above illustrate a concept that continues to ring true across the legal industry: having the optimal mix of people, process, technology – and now legal business intelligence – is key to successful transformation. While successive generations have tackled each of these in turn, the latest involves all three with a particular focus on data and insights. When looking for a strategic partner, find a third generation ALSP that takes this holistic approach. They will offer best-in-class solutions unified in a cohesive and integrated architecture of people, process, and technology. These ALSPs realize that to address the challenges of today's corporate legal department, technology-alone or people-alone solutions will be insufficient.

Looking Forward

A 2023 report by Thomson Reuters Institute found that the ALSP market has grown by 145 percent since 2015. According to the report, at the end of 2021 the ALSP market was valued at roughly $20.6 billion, the result of a 45 percent increase in two years. This is forecasted to keep trending upward as ALSPs focus on synthesizing people, process, and technology to guide clients on their legal transformation journeys. When partnering with ALSPs to help get work done, consider the additional value a third generation ALSP can provide through the creation of actionable legal business intelligence.

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.

CLOC'ing the Speed of Transformation

Over the past decade, there has been substantial transformation within the legal industry, but it has not been at rapid speed. The 2023 CLOC Global Institute asked the question: will this year be different due to all the hype around generative AI tools? The largest group of legal operations professionals to date gathered in Las Vegas last week to explore this and other industry questions.

The consensus? There is definitely a split. Some are bracing for accelerated transformation and others think that change will occur but continue to be incremental. No matter where an organization may fall on this spectrum, one thing for certain is that technology is changing the way the legal industry works. What is unknown is the rate and velocity at which this transformation will occur.

Below are two ways that legal operations professionals can prepare and proactively plan for industry trends that will affect process, tech needs, and client demands.

#1: Understand the state of legal innovation

For something to transform it needs to undergo significant change from its previous state. The legal industry has experienced several periods of transformation through the years, from digitization to legal tech adoption. This has altered how legal professionals get work done, strategize, and advise clients. While organizations have been using AI for years, the rise of generative AI tools has brought on a new level of risk.

At CLOC, there was talk of the age-old fear that attorneys may be replaced by machines, and their uncertainty around how to use new tools safely and strategically. Some think that AI will replace the need for document management and knowledge management jobs, while others believe the fields will change, but others firmly disagree. The overall tone was that legal operations professionals need to help lawyers overcome this fear but allow them to embrace the notion that it is okay to be hesitant when new tools enter the market. This has happened in the past and the industry has adapted and continues to innovate. Above all, this tech will not make legal professionals

obsolete and cannot replace legal judgement. There is still a human component needed to train and review knowledge or document management processes. Technology advancement instead brings the opportunity to change the definition of legal innovation and discover better ways to work and use these tools beneficially both within and outside the legal department.

Additionally, CLOC attendees were reminded that transformation is not a linear and predictive process. Regardless of where an organization's viewpoints fall regarding the speed of transformation, until implementation and adoption spreads this is unknown. Teams can consider their unique needs and risk tolerance before deciding whether to alter processes or invest in new tools.

#2: Leverage community – both peers and experts

With change approaching, legal operations professionals are left seeking the best way to navigate a new frontier. This is where the importance of community comes into play, which CLOC offers. The institute's keynote speaker discussed "how to citizen," which requires showing up, investing in relationships, understanding and harnessing power, and seeing the value of the collective. Legal operations professionals that uphold these pillars can derive benefits on their transformation journeys.

CLOC attendees had a place to discuss the state of the industry, anticipate changes, and make connections to tap into after the event. This allows people not to feel alone and presents opportunities to learn from one other, consider differing viewpoints, and discuss solutions to challenges.

There are several ways to leverage this community. Talk to a peer from another organization dealing with similar obstacles to get insights into successes and failures. Tune into industry webinars and podcasts to learn more about emerging tech such as generative AI or updated contract lifecycle management (CLM) solutions. Create a peer group that meets every quarter to bounce ideas off one another and discuss market trends.

In addition to leveraging peers, turning to experts is a valuable and collaborative way to navigate transformational periods. Third generation ALSPs are the most advanced category of providers that are valuable resources. They leverage process optimization principles to make improvements to legal business performance and consult on legal operations issues. They are researching, using the tech, and assessing risk. They can help predict when the AI wave will peak and throw out lifesavers so legal professionals can stay afloat and embrace new solutions safely and beneficially. These experts can also advise on how to craft and leverage metrics as proof points to illustrate ROI and foster buy-in from an enterprise. Even for those not ready to embrace tools like generative AI, it is critical to have a partner that can vet the tech, monitor competitor moves, and advise on potential use cases down the road.

Conclusion

The takeaways from CLOC were three-fold. First, the industry is approaching a significant period of transformation. Second, whether anticipating vast or incremental change, whether your organization is tech curious or tech careful – now is the time to lean into community. Lastly, understanding the value that comes from leveraging peers and experts is crucial to staying ahead of the curve. Having the right knowledge and partnering with the right people will place legal in a better place to invest in optimal tools and demonstrate value to the enterprise. It will also make this period of transformation a little less scary and a little more manageable.

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.

BYOD in 2023: Regular Evaluation Can Help Reduce Risk

Is it time to revisit your organization's Bring Your Own Device (BYOD) policies? The answer to this question is subjective, but doing so can be beneficial as the workforce and productivity behaviors change. Having a BYOD program allows employees to conduct business on their personal devices, which can save an organization money and foster flexibility. CBS News cited that most – 67 percent – U.S. workers conduct business over their personal phones, which includes instances where there is no formal BYOD policy in place.

Over the past few years there has been a rise in remote working while technology continues to advance. There are more applications than ever before to communicate through or store data. This creates cyber, privacy, and legal risks associated with conducting business on personal devices. Due to this increased risk, it may be time to change gears.

BYOD Evaluation Checklist

If an organization currently has a BYOD program or is thinking about establishing one, consider assessing these five components:

1. **Business applications:** Along with the popular business applications such as email, calendar, and Teams messenger – there are a variety of other apps available to conduct business. This is where organizations need to clarify what is acceptable under their BYOD policy to avoid security breaches. A 2022 survey by Helpnet reported that 57 percent of employer respondents were concerned about employees downloading unsafe apps or content.

   Can employees connect directly to the company server? Are text messaging or cell calls allowed – or should all business communications be handled via Teams, email, or other approved communication apps? How can organizations enhance security for authorized apps and monitor compliance with the policy? These are a few key questions to address and reassess as new technologies enter the business sphere.

2. **Cyber controls:** Security is the top priority in a BYOD program, which was confirmed by the same Helpnet survey where 63 percent of respondents reported data leakage as their top concern. Some factors to consider are integration capabilities, unsupported or unsecure networks, lack of passwords or two-factor authentication on devices, malware, updates, and physical theft.

   To reduce risk, the first place to start is having a robust policy covering everything from accepted applications to data storage instructions. Employees need to receive copies of the policy and any subsequent updates, along with regular training on acceptable practices. Enhanced passwords such as two-factor authentication, articulated procedures for lost devices including the ability to data wipe, and solid IT support are all helpful controls to manage security risks present in a BYOD environment.

3. **Regulatory applicability:** The regulatory landscape is expanding, especially in the context of consumer privacy. This means that employees who handle personal data as part of their job need to be cognizant of this when using a personal device. Employers may consider banning certain functions involving sensitive information on personal devices or take extra measures to secure that data. Failure to do so could result in violation of applicable privacy laws and increased liability in the event of a data breach.

4. **Litigation exposure:** When data lives outside company walls, it can still be discoverable. All communication and files are potentially discoverable if deemed relevant and unique, even over personal devices. Employees need

to be aware of litigation hold potential. This is why it is extremely important to have clear boundaries around which applications are acceptable, as the failure to do so could result in collection of text messages or other apps where personal and business data are intertwined. Over-collection can also be expensive and defeat the cost-saving aspects of having a BYOD program. Generally, collection from an enterprise level chat application is performed at the server level, so personal device collection would not be necessary.

With the rise of personal device usage in the remote working era, courts have recently addressed the issue of who controls data stored on an employee device. Take the case of In re Pork Antitrust Litigation, No. 18-CV-1776 (JRT/HB), 2022 WL 972401 (D. Minn. Mar. 31, 2022) as an example. Here, the court found that employer control over text messages was lacking. The absence of clear ownership over texts in the BYOD policy meant that the employer could not demand access to these messages. This provides notice that the wording of a BYOD policy is crucial and will guide potential disputes.

5. **Supervision:** A BYOD program carries an inherent level of trust, as it can be more difficult to monitor compliance when employees are conducting business off-premises on their own devices. With the complexity and breadth of new digital applications entering the market, this may be enough risk for organizations to decide that BYOD is no longer acceptable. However, many will likely still find the benefits to outweigh the risk and those organizations will need to rethink new ways to supervise compliance. This can be tricky as employers will want to avoid encroaching on the personal aspect of their employees' devices, but requiring business take place only in the cloud or over company applications is a good place to start. If conduct outside this policy occurs, it is important to have a check-in to realign expectations and avoid consequences.

Projections

When balancing business benefits against risk, it is difficult to predict what the future holds for BYOD programs. It is a safe bet that more organizations will start implementing formal policies and increase supervision. This will require individualized risk analysis and be dependent on the technology available and authorized. Information governance and data security challenges will continue to evolve. The courts will also play a key role in further addressing possession, custody, and control. Organizations need to remain cognizant of all these developments when determining whether BYOD is acceptable and what constraints to implement.

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.

Deepfakes Bring Deep Risk

Most people know what a deepfake is but have not put much thought into how it could affect business operations. Deepfakes are videos, pictures, or audio that have been convincingly manipulated to misrepresent a person saying something they never said or doing something that they never did. Machine learning tools make connections between the subject's physical attributes, sounds, and other unique identifiers to create extremely realistic outputs. Historically, deepfakes were used for things like movie dubbing. Now, cybercriminals use deepfakes maliciously for various reasons from impersonating political figures to scam attempts.

But how worried should organizations be about falling victim to deepfakes and what are the potential repercussions? Analysts would say to be very concerned, with 66 percent of participants in a 2022 VMware survey reporting that their organization experienced a deepfake incident. This year was a 13% increase over the year prior, a significant leap over a short period of time. Organizations should include the risk of deepfakes in their cyber readiness initiatives if not doing so already. Proactive planning prior to an incident can save precious time and ensure smooth service delivery when it counts most.

Risk Analysis

To appropriately evaluate risk, it is key to understand how certain attacks can infiltrate and affect an organization. Cybercriminals can access public company data and make changes or synthesize new content.

Here are examples of how deepfakes can materialize:

- Using manipulated audio to sound like a direct manager, member of the legal team, or client to deceive that person into revealing sensitive information. This could lead to a data leak, fraudulent financial transactions, and more.
- Creating a fake video or audio recording of a C-Suite member to paint the organization in a bad light or make statements that do not align company culture, product launches, or that otherwise damage reputation.

- Enabling various phishing campaigns and business email compromises.
- Perpetrating fake interviews, taking a licensing examination under a false identity, or bypassing authentication controls to access personal identifiers or sensitive business data.

The types of losses to anticipate with these types of security compromises are financial and reputational. It can be hard to detect the losses as more threat actors of every sophistication level learn to create deepfakes and when employees are not educated about the risks of these attacks. Even after proven false, damage occurs and sometimes it is hard to overcome the mistrust, rebuild image, or execute necessary financial mitigation. It is crucial to understand threat potential and evaluate how much damage a deepfake could cause in order to prepare accordingly.

Remaining Cyber Ready

Clear information governance, cyber incident investigation, and data breach response plans are critically important to limit the consequences that could result from a substantial data breach. Deepfakes and other trending attack methods carry not only cyber risks, but also legal risks. Failure to safeguard certain data can result in regulatory violations, contractual defaults, and other legal exposure.

Below are three ways organizations can mitigate the risk of a cyber incident involving deepfakes and be more prepared in the event one transpires:

1. Partner with a service provider that can provide both proactive and responsive services. This may include reducing the volume of data stored internally in a legally defensible manner; creating, evaluating, and assessing the organization's cyber incident response plan; and leveraging AI tools that can identify deepfakes.

2. Educate employees about the existence of deepfakes, how to spot an attack, and reporting protocols. Also ensure that company leaders, legal, finance, and IT staff have extra education on this topic.

3. Deploy extra security measures such as a detailed unique process when dealing with money transfers, restricting access to personal data and trade secrets, monitoring social media and news outlets for mentions, and utilizing identity verification technologies.

The most important thing to remember is that even a small amount of preparation will go a long way and can help save an organization's reputation, business, and assets. With deepfakes, what was once akin to a prank phone call can now be used as a powerful tool to defraud and damage individuals and businesses. Organizations must have dedicated personnel and external partners to keep up with the evolving threat landscape and deploy strategies and tools to mitigate risk.

While no organization can eliminate cybersecurity risk, applying professional teamwork to the problem can lessen the blow. In today's digitally driven world, breaches will happen. Having professional staff and outside partners with the right knowledge and resources is the key to advancing good cyber health and remaining compliant. Cybersecurity is a work in progress requiring teams to constantly improve cyber compliance 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.

Correlating Commercial Real Estate and Bankruptcy Trends

Is the U.S. commercial real estate market in a bubble about to burst? Several financial market analysts would answer this question with a yes, it's more likely than not that the sector will experience some significant financial distress. Commercial real estate has not rebounded in this post-pandemic economic environment, inflation continues to rise, and interest rates are climbing upward. Demand for office space has been significantly reduced as companies reassess and realign their office space needs. It appears that some form of hybrid work will remain for a significant percentage of the workforce. As a result, commercial bankruptcies are on the rise. Per Epiq data, March 2023 commercial bankruptcy filings were 79 percent higher compared to March 2022. Additionally, analysts have reported that followed by a quick deflation – the $2.9 trillion in commercial mortgages due will need to be renegotiated in the next two years. The current dynamics indicate that a financial crisis affecting the commercial real estate market is on the horizon.

But is the commercial real estate market in a bubble? By definition a bubble is an economic cycle that is characterized by the rapid escalation of market value, particularly in the price of assets. This fast inflation is quickly followed by a quick decrease in value, or a contraction, that is sometimes referred to as a "crash" or "burst bubble". Values of commercial real estate have decreased as the need for office space has been significantly reduced. It doesn't appear that this crash will create a financial crisis but rather, it will add distress to an already recession-like environment.

Market Conditions

BankruptcyData.com indicated that real estate companies are prime candidates to seek bankruptcy protection. As noted, rising interest rates coupled with hybrid work are the two main factors affecting the market. Let's dive into this a little deeper.

Interest Rates

As a response to inflation, the U.S. Federal Reserve has significantly raised the benchmark interest rates to over five percent. To provide some context, these interest rates were

close to zero percent in the beginning of 2022. Regional banks have also experienced more pressure to impose stricter lending requirements. Currently, property values have plateaued and the cost to borrow money has gotten much more expensive.

Remote Work Trends

Hybrid work models are the new norm for most companies in the United States. This has created an opportunity for organizations to transform operations in order to continue successful operations, maintain revenue streams, and create a positive company culture accounting for varying working styles. To stay afloat and meet these evolving needs, organizations are reimagining the role of the physical office.

New working models incorporate shared spaces, downsizing, or eliminating the physical office altogether. Because of the declining commercial occupancy, there is less of a market demand for traditional real estate spaces which affects the stability of the real estate market. However, there is a growing need for shared or short-term rental spaces. Many organizations want access to commercial spaces on a demand basis and ready for use, which could create a new market opportunity to fill gaps created by the decline in more traditional commercial occupancy.

Illustrations

Some examples of how these variables are affecting the commercial real estate market include:

Many analysts have focused on New York City, one of the largest concentrated areas of commercial real estate in the U.S. Several are bracing for a challenging period for commercial real estate.

- A major real estate firm reported that the office space vacancy rate in New York City has grown over 70 percent since the beginning of the pandemic.
    - The largest landlord for office space in New York City experienced $93 million in net losses in 2022, which is a drastic change from the $435 million in net profits experienced over 2021.
    - Researchers noted that due to the shift to remote work, the stock value of several New York City commercial real estate companies has declined on average by 32 percent in 2020.
    - According to a commercial real estate analytics company, over $17 billion in mortgage bonds that are backed by commercial real estate are due in 2023. This figure continues to grow as the market values decline.
- According to public records, an investment management company ceased payment on a $325 million loan backed by an office building in Las Vegas.
- A real estate firm recently purchased an office campus located in the Chicago suburbs for under $20 million. It was recently sold for $74 million in 2018, demonstrating a significant drop in value. The property, like many others, was experiencing declining occupancy rates due to the rise in hybrid work models. The firm plans to repurpose the space.

Predictions

Based on the current state of the real estate market, here are four predictions of what might come:

- The crash of the commercial real estate market is near and will compound an existing distressed cycle as interest rates continue to climb. Less occupancy resulting in defaults on leases and less renewals will lead to a greater need to refinance. However, refinancing will be challenging as interest rates are projected to keep rising.
- Real Estate Investment Trusts (REITs) will become distressed. REITs are companies that own and operate commercial real estate that produce income, generally from rental payments. Office buildings, shopping centers, and hotels are prime examples. When larger businesses turn to bankruptcy – like what is happening with Bed, Bath, and Beyond – then REITs are losing a big chunk of their rental income.
- Commercial real estate bankruptcies will increase over the next two to three years. As noted, filings have already increased this year and market conditions will drive more activity in this space.
- To rebound from the decline in commercial real estate values, investment firms will explore alternate ways to utilize existing office space. To increase occupancy rates, owners need consider whether they should convert their existing space to align with our new hybrid work environment. There will be more short-term rentals, hoteling services, desk rentals, and shared spaces. Converting commercial office buildings to residential use is expensive due to construction costs, planning and zoning approvals, and negative tax ramifications. Alternative uses for commercial space will also emerge including laboratories to support life sciences and teaching facilities.

Will these predictions ring true? With the ever-evolving state of the commercial real estate market, it is likely they will. Those affected should watch for how interest rates and remote work trends continue to affect the market, and the continuing role of bankruptcy to help navigate

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.

Legal Ethics and Emerging Technologies

The phrase "emerging technology" has long become repetitive across the legal industry – and beyond. Email, chat, simple automation software, and TAR were all in this category at one point. The difference now is that the legal industry is experiencing an accelerated period of transformation where technology is advancing at record speed. Legal professionals are figuring out the best way to utilize and advise clients on tools such as generative AI. This creates both excitement and skepticism, as lawyers need to evaluate risk appetite and integrate strategies.

It is crucial to factor ethics into any changes in workflows and practice habits. While change is necessary and beneficial, it must be done carefully to avoid ethical violations that could provide reputational harm not only to the lawyer, but also the organization. This includes remaining informed on new American Bar Association (ABA) and state bar rules and opinions, as well as industry best practices. Given the prevalence of remote culture in business along with legal's foray into modern law, it is safe to anticipate updated guidance in the coming years. But for now, lawyers should look to the existing rules to guide behaviors with this and other emerging technologies.

Key Obligations

When dealing with emerging technologies, one of the first questions to ask should be: what ethical duties apply here? Confidentiality and competence are two major duties that surface with tech usage. Keeping client data confidential requires an extra layer of vetting to ensure all tools used in-house and via third parties are secure and protect sensitive client data. To remain competent, lawyers must keep informed about innovative trending technologies and basic features even if not utilizing these tools. This has materialized with AI usage in legal practice, most notably the role of technology-assisted review in litigation and investigations.

Without maintaining confidentiality and competence in situations like these or holding onto the unwillingness to adopt emerging technologies, lawyers can put client data at risk and even inadvertently provide disadvantaged

representation. Failure to uphold these and other ethical standards can result in discipline, disbarment, court sanctions, reputational harm, and client distrust.

Generative AI and Legal

The use cases for AI in legal practice have expanded as the tech has matured. AI can assist with document review, settlement evaluation, litigation analysis, internal investigations, regulatory compliance, and strategy decisions. With generative AI tools like ChatGPT trending, it is crucial to understand the different risks present and how to safely and integrate usage into legal practice. Here are three factors to consider.

- **Confidentiality:** Putting confidential client information into a large language model like ChatGPT can open the door to waive privilege and can violate the attorney-client relationship. Any information included in a prompt will not be deleted and can be used for training purposes.
- **Factual Discrepancies:** AI services may create untrue facts or leave out citations, but still appear convincing. This can result in violation of a lawyer's ethical duty not to make false statements to the tribunal or third parties. While this is not barring use of generative AI for brief or memo drafting, best practice dictates review of the facts to ensure they are accurate before filing with the court or transmitting to opposing counsel.

- **Data Security:** ChatGPT's security risks have already made headlines. There have been unintentional leaks of trade secrets by employees using it for everyday tasks, a ChatGPT data breach exposing private information, questions about non-compliance under privacy laws like GDPR, and even bans by data protection agencies. Lawyers must consider data security when deciding whether to use generative AI for document review, contracting, language translation, and other use cases that involve confidential information. Keep monitoring any changes that materialize following incidents and whether in-house capabilities emerge.

Staying informed of the considerations above will keep lawyers competent when making decisions about using generative AI and advising clients. Also, do not discount the obligation of client communication that would mandate consent before using such tools for a case.

Conclusion

While the intersection of emerging technologies and legal ethics will continue to evolve, being mindful of the basics can help lawyers keep their duties to clients. The business world is changing and legal is embracing digital transformation. The areas discussed above are only a snapshot of key duties lawyers must be mindful of when incorporating emerging technologies into their practice, and there are many unknowns with innovative tools, such as generative AI. As these technologies mature, more will be known. In the midst of innovation, it is also important to remember that simple communication channels used daily such as email and text can inadvertently open the door for unethical behavior if not used carefully. The ABA, state bars, and courts will help clarify what it means to be ethical in all these instances.

For additional reading, please download the whitepaper: Legal Ethics in the Digital Age

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.

Using Legal Data to Enhance Relationships

Taking a business centered approach to legal issues continues to grow in practice. Modern law is here to stay, which encompasses the act of embracing emerging technologies and new partnerships to increase efficiency and make smarter operational decisions. Data is increasingly at the center of reshaping strategy, and teams that can tap into deeper intelligence offered by this data are filling gaps and expanding capabilities.

The instances where data can drive better outcomes continues to expand. For example, a recurring question amongst practitioners is how law firms and corporate legal departments can collaborate more effectively. This has been an uphill battle for decades. The good news? Data can help here too. These relationships can be greatly enhanced if both become more data driven.

There has been a recent shift to view the legal team as one unit that encompasses not only law firms and corporations but also service providers that assist with matters and tasks. More firms and legal departments are shifting the way they use data. They are focusing on value instead of fees and tapping into deeper insights that drive meaningful transformation across the board. But where to begin?

Reimagining Data Analysis

When not siloed or underutilized, data has been traditionally used to either justify or cut fees associated with work that outside counsel performs for their corporate clients. While these are solid insights to track, looking deeper into why a certain workflow or tool is not performing allows a more holistic approach that targets underlying issues.

Now, industry leaders are finding ways to create organizational advantage through the power of legal business intelligence. This is changing the data conversation from cost reduction to value, which is powerful and will alter the way teams collaborate. This positions alternative legal service providers (ALSPs) as a crucial part of the modern legal team – especially those that can pull data from a variety of sources into a single repository and output true legal business intelligence. Making all legal data accessible and actionable allows corporate

counsel, and the firms that advise them, to see where they need to direct or optimize legal work and resources.

Here are three examples of how corporate and outside counsel can collaborate and derive valuable intelligence from data to inform strategy, partnerships, and future investments.

1. Law firms hold so much corporate data that just sits in storage such as contracts, legal advice, and supplier agreements. Being able to extract this information and put it back in the hands of corporate clients offers several advantages. First, firms can use this as a business development tool that sets them apart from competitors. Second, it empowers corporate legal departments to own their own data and tap into insights they may have overlooked. Lastly, both teams can look at this information together to pinpoint gaps and decide what metrics to track.

2. Firms and legal departments can strategize which data to capture that would allow corporations to justify pricing models or legal project management decisions, and ultimately retain their clients. Examples include information about the performance of a new AI tool for automating and streamlining portions of document review or how partnering with an ALSP offering flex

attorneys regularly cuts costs on legal matters and yields more settlements. Synthesizing these data points can demonstrate cost- savings and justify investments.

3. Law firms can track market trends and use proactive forecasting tools to provide actionable intelligence to their corporate clients. More legal departments are looking to go past the usual dashboard metrics and uncover data that answers questions they did not even know they had. For example, using regulatory horizon scanning can inform when a law change triggers an organization's compliance obligations. These tools can synchronize with internal contract management repositories, policy documents, and other relevant systems.

With so many regulations that legal organizations and their clients need to monitor, it is crucial not to let things fall through the cracks. Having this information not only allows proactive tracking, but also the opportunity to sharpen information governance policies.

Using data more strategically not only improves collaboration efforts, but also strengthens risk assessment and ensures each part of the modern legal team is performing to their full potential. It also shines light on opportunities to expand ALSP relationships and shift technology priorities.

Embracing the Journey

It can be difficult to decide where to start on this journey, but having a framework in place is the key to creating a data-driven culture. While capturing, consolidating, and quantifying data are all components of this framework – communication is the element that ties it together. Change management requires regular communication between law firms and corporate counsel about how to measure value. From a new metrics solution to bringing in strategic ALSPs as consultants, the possibilities are plentiful. The focus should be on how to identify competencies within data that can inform new and better workflows.

Starting with small data strategies and scaling up is the best way to accomplish this, especially with established law firms housing enormous amounts of data ready to convert into business intelligence. Have a conversation and go from there. What are the urgent business requirements? How can teams go beyond layering tech over data and derive value? These are just a few questions to explore. Turn to consultants for recommendations on platforms that will capture and consolidate data, advice on how to generate legal business intelligence, and solutions that improve data management efforts. Coupling these efforts with market trend monitoring can help legal organizations better understand clients, optimize the supply chain, and make data-driven decisions that transform their approach to legal practice.

To learn more, watch our latest webinar co-sponsored with Centaur the Lawyer.

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.

Fireworks Aren't the Only Explosions This Summer - ALSP Market Growth Is Lighting up New Opportunities for Legal

It's that time of year again! Fireworks are lighting up the sky and captivating audiences that gather to see what the display holds. A similar show is happening in the legal industry with the Alternative Legal Service Provider (ALSP) market. This is driven by greater focus on efficiency, desire for general counsel to run legal like a business and evolving legal tech solutions. There has also been more willingness from law firms to explore formal ALSP agreements.

The legal industry is in a state of transformation and exploring new solutions to longstanding challenges such as information governance, document review, and compliance obligations – to name just a few. ALSP competencies have evolved alongside legal technology sophistication and the use cases are a mile long. Think legal technology consulting, managed services, data breach response, contracts management, outside counsel cost control, compliance, and so much more.

The Rapid Growth of ALSPs

Thomson Reuters Institute recently released "Alternative Legal Services Providers 2023: Accelerating growth & expanding service categories," which contains compelling statistics and commentary on the reasons for market changes. Take a look below.

- The ALSP Market has grown by 145 percent since the first report of this nature was issued in 2015, with the most growth happening over the past two years.
- The report's position is that the rapid growth is a result of numerous factors including "stronger appreciation for the capabilities of ALSPs, such as their access to specialized expertise, ability to introduce efficiencies and control costs, and the flexibility they allow law firms and corporations in managing their headcount." Additional external drivers noted included the increasing comfort level for remote work and the need for law firms to have a partner that can consult on legal technology. These sentiments are reflected throughout the legal industry and illustrate that having a partner able to offer flexible and customizable services is valuable.

- At the end of FY 2021, the ALSP market was valued at approximately $20.6 billion, which represents a 45 percent increase in two years. The compound annual growth rate for FY 2020- FY 2021 was also up five percent than the prior two years.
- For the largest U.S. law firms surveyed, 26 percent plan to increase ALSP spend. For U.S. corporate legal departments respondents, this figure is similar at 21 percent.
- The ALSP use case amongst law firms that experienced an impressive leap was legal technology consulting. 51 percent of large firms, 37 percent of midsize firms, and 31 percent of small firms cited this as a reason they use ALSPs.
- For U.S. corporate legal departments, the top use case was regulatory risk and compliance services. 50 percent of respondents reported this as a use case, which represents a five percent uptick over the last two years. A new top use case in this report that made it to spot number three was eDiscovery services. This use case shows the most growth (16 – 28 percent) over two years correlating with accelerated digital transformation in the legal industry. The other use cases making the top five list were legal research services (48 percent), contract management and abstraction (26 percent), and intellectual property management (24 percent).

- The report also analyzed top trending use cases in legal departments outside the U.S. In the U.K., intellectual property management is at the top. In Canada, specialized legal services was reported as the top use case. In Australia, legal research came in first on the list.

This is just a snapshot of key statistics illustrating growth. The report takes a deeper dive into trends in both the U.S. and globally. Overall, the survey showed that there was increased interest across the board to keep using ALSPs, expand services, and venture into a partnership for the first time. Those not using ALSPs in both the law firm and corporate setting cited their top reason as preference to keep the work in-house. Other reasons included service quality concern, lack of cost reduction, data security concerns, and diminished awareness. It is important to note that the data security response use case experienced a significant jump in the last two years from 16-31 percent. This reflects the industry trend of investing more in cybersecurity, breach response, and cyber preparedness initiatives. With more ALSPs expanding capabilities and tapping into legal business intelligence, these reasons will likely be bumped in future industry studies.

Opportunities and Predictions

Will the ALSP market continue to skyrocket and light up the legal industry? All signs point to yes, as they are becoming more integrated as a staple of the organization. Not only corporate legal departments, but also law firms, have sought out and expanded partnerships with ALSPs in recent years. The sophistication of these providers has resulted in access to several benefits. This includes specialized expertise, better strategies around cost management, access to innovative legal technology, retention management, enhanced data security, and improved compliance. As the Thomson Reuters report pointed out, these are some top reasons driving market growth in recent years.

What it comes down to is finding the optimal mix of people, process, technology, and legal business intelligence to keep up with industry demands. The roles of the modern legal team are not clear cut and require collaboration between all members to reach the most efficient outcomes. This is where the recent generation of ALSPs have taken center stage, as they offer best-in-class solutions unified in an integrated architecture of people, process, and technology.

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.

Nothing to Fear Here – Using AI Tools Responsibly Breeds Success

The news is flooded with stories about artificial intelligence (AI) tools -- some shining light on the benefits, and others meant to invoke fear and panic. While the latter has bred some skepticism about AI usage in business, it is time to take a step back and look at what drives the errors. Oftentimes, it is not the tool itself but instead the human behind the tech. The reality is that many organizations are using AI highly successfully and without mishap.

Every organization – regardless of what industry it may operate in – should understand how to utilize AI in a safe and responsible manner. Most are likely already aware of the usual risks present in AI tools and other emerging technologies. Inherent bias, cybersecurity gaps, and lack of transparency are a few examples. However, many are forgetting to factor in the human component. It is crucial to understand the benefits and risks of both human and technological contributions to changing workflows. This helps teams build strategies and systems that realize the best in both, while effectively managing potential downsides.

AI in the News

A notable AI story in the media recently has been about the New York lawyer who used ChatGPT to help draft a brief that went south. The output included convincingly cited cases that did not in fact exist. Opposing counsel discovered the false citations and brought the issue to the court. The lawyer used ChatGPT to verify the accuracy of the decisions and the tool ended up creating facts and attributing the existence of the cases to legal research search engines. The lawyer responded that this was his first time using ChatGPT as a supplement to legal research and he was unaware that the tool could create false information.

In this case, the court recently imposed sanctions including a $5,000 fine that was joint and several among each counsel and their law firms, and an order to write to each judge who had been falsely identified as the author of the fake opinions, and to provide them with the transcript of hearing before the court, including copies of the fake opinions.

Since this incident, two federal judges are requiring counsel to submit generative AI certifications when submitting a document to the court. Counsel must attest that they did not use generative AI or that they used it and had a human check the information for accuracy. Legal analysts across the country have spoken freely about this decision, some calling it unnecessary overkill and duplicative, and others finding it necessary due to the new risks present in this technology.

Other instances of "scary" AI in the news include stories about using this tech for negative scientific purposes and predictions that AI will replace jobs. While headlines like these can increase fear about using these tools for business purposes, there are just as many stories on the other side of the coin that explore the benefits of AI and look at how responsible usage can limit risk.

Using AI Responsibly

From reducing documents in a dataset to facial recognition software and HR recruitment tools, AI has proved very beneficial across industries. With generative AI on the scene, organizations are considering how this tech can also benefit their businesses. It is crucial to examine both benefits and risks to pinpoint best use cases. In many instances, the benefits will outweigh the risks and there are best practices to employ that will curb fear. Learning how to use these tools safely and responsibly is the key.

Staying educated is the most important way to use AI responsibly. Keep up with news about things going awry and use it as a learning experience. For example, in the case law example above the lawyer could have mitigated risk much earlier if he would have initially checked the sources and not subsequently use ChatGPT to justify the research. Simply going into a legal research database after using generative AI as a starting point would have brought the fake cases to the lawyer's attention and avoided potentially sanctionable behavior. The fact that the lawyer used ChatGPT was not at issue here, it was the manner in which it was used. The responsibility to fact-check and provide quality control on the technology's output will always remain the responsibility of human lawyers. Lawyers must remain technologically competent and check their work or will otherwise face court sanctions, ethical violations, reputational harm, and lost business.

Turning to the fear of job loss, a recent Goldman Sachs report indicated that AI could replace 300 million full-time jobs. This is the type of news that raises alarm at first read, but it is prudent to point out that even when tech has "replaced" jobs in the past it has opened up new roles and different opportunities. AI is currently being used in most industries as a supplemental tool and the human component is still necessary but may just look different.

It is also crucial to remember that there are more generative AI tools available than ChatGPT. Tech companies are creating systems designed for specific industries or that can be privately used within an organization's own infrastructure.

Conclusion

The takeaway here is that generative AI can be just as beneficial as the next tool when organizations consider the human component and use it responsibly. Delegate tasks wisely with a deep practical understanding of the limitations as well as the advantages of all the different resource options for delivering services, both AI and human. Doing so will allow organizations to reap the game-changing benefits that technology offers with confidence. Considering all the hype, more AI regulation is definitely on the horizon. Organizations must continue to monitor developments in this area and implement policies regarding appropriate tech usage for business tasks.

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 EU-US Data Transfer Framework Finalized: What Does the Future Hold?

With data privacy landscapes changing around the globe, how can organizations handle cross-border deals while still remaining compliant? This has been a burning question over recent years.

It is common for organizations to have a global presence or conduct activities in several countries. The need to set up data transfers involving areas subject to strict regulation, such as the EU's General Data Protection Regulation (GDPR), has created obstacles. An updated framework for data transfers between the U.S. and EU was recently finalized. Affected organizations must understand how this change materialized, new requirements imposed by the framework, and what analysts predict for the future of EU-U.S. data transfers.

The History

For almost 25 years, the EU and U.S. had some type of agreement in place to expedite data transfers while maintaining adequate protections. When the GDPR drastically changed the EU's privacy landscape, significant revisions to the data transfer process were necessary. Take a look at the timeline:.

- In 2000, the EU-U.S. Safe Harbor Framework was established to allow cross-border transfers. It was deemed invalid in October 2015.
- In July 2016, the new Privacy Shield framework became effective.
- In July 2020, the landmark Schrems II decision came down and invalidated the Privacy Shield framework due to diminished privacy protections violating the GDPR and apprehension over U.S. surveillance during transfer activities. The EU proclaimed it did not recognize the U.S. as having adequate data privacy safeguards in place.
- In June 2021, the European Commission created new standard contractual clauses (SCCs) that enhanced accountability and transparency. The SCCs apply to personal data transfers from EU member states to other countries and ensured cross-border activity aligned with GDPR standards.
- With the Privacy Shield gone, organizations have turned to the new SCCs to carry out EU and U.S. data transfers. This is a more complex and unpredictable mechanism that requires time-consuming data transfer impact assessments.
- In March 2022, the EU and U.S. reached an agreement in principle to implement another mechanism for transfers that would streamline the process, allow for self-certification, and enhance privacy protections.
- In October 2022, President Biden signed an executive order outlining the steps to officially implement the new framework, once again mentioning self-certification and increased oversight over data transfers.
- On July 10, 2023, the European Commission finalized the adequacy decision under the new EU-U.S. Data Privacy Framework, claiming that the provisions applying to U.S. surveillance and consumer redress were satisfactory.

The New Framework

The U.S. Department of Commerce will run the new EU-U.S. Data Privacy Framework program. It is not mandatory, and organizations can choose to use other mechanisms like the SCCs to effectuate transfers instead, but this framework will streamline the process. Here are the key features:

- Organizations must publicly declare they will comply with the proscribed privacy obligations during transfers. This includes data minimization, data sharing limits, and more. Doing so provides the Federal Trade Commission jurisdiction over enforcement, if necessary.
- Organizations must provide GDPR-like protections to individuals so information can flow without advancing extra security measures.
- To address surveillance concerns, there are now limits on when certain agencies can access information coming from the EU, increased oversight, and establishment of an independent redress process.
- Individuals can file complaints with their own domestic data protection authority to address suspected information mishandling. After that, there will be additional layers in place to transmit complaints to the U.S. for investigation, review, and resolution before a new Data Protection Review Court. This redress process will also be available for transfers occurring outside of the new framework, including the SCC method.
- The EU will provide ongoing review of the program to ensure it maintains adequacy status.

With this, organizations can now take steps to self-certify under the new framework. While many have been waiting in limbo, some have chosen to maintain certifications under the invalidated Privacy Shield even though not in use.

Forecasting the Future

With this being the third attempt to implement a streamlined data transfer mechanism, there are two questions on everyone's minds. Will it stick this time? And if the new framework is struck down, what will be enough? Analysts are torn and opinions are all over the board.

The leader of the Schrems case has already proclaimed that he does not think this framework is valid and intends to bring a court challenge. The European Parliament and other data protection authorities have concurred. Skeptics believe there is a need for legislative action by Congress to change U.S. surveillance law to provide added protections.

On the other side, the European Commission President recognized that the new framework contains unprecedented commitments that will facilitate safe and secure transfers. But will this ring true? Only time will tell.

In the meantime, some analysts are urging organizations to take advantage of the framework to alleviate the burden carried over the past three years. Others are advising that they be more cautious, consider new compliance obligations, and perform risk analysis before moving forward.

Regardless of the path chosen, keeping track of new developments should be top of list. A court challenge will likely take years to play out and with the industry split on this issue, there is uncertainty how the ruling will unfold. In the meantime, how U.S. organizations put forth compliance efforts and forthcoming decisions from the new Data Protection Review Court will shine more light on the fate of the latest EU-U.S. Data Privacy Framework.

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.

Antitrust and Global Investigations: The Era of the Legal Technologist Has Arrived

The marriage of technology expertise with the license to practice law is in high demand and essential to the efficient handling of large-scale and complex antitrust and white-collar investigations and litigation. This is no longer a discretionary skill set designed to benefit those who respond to ESI requests, but rather a necessary proficiency needed to navigate the eDiscovery landscape. As electronic communication volumes grow and litigation and investigations continue to increase, the efficacy of conducting a linear style document review becomes highly questionable. Faced with a costly and time-consuming process, the option to engage a "legal technologist" who can quickly get answers and efficiently identify the most critical records will shape a new frontier. Attorneys committed to the practice of law and adverse to technology can remain firmly entrenched in their preferred practice and rely upon experts to drive the technology and analytics component. Any firm responding to a discovery request should develop a trusted partnership with a provider that can supply this critical service. This relationship rises above simply "contracting" out, due to the significance and value of the role. These legal technologists are not just outsourced resources, but valued consultants who should be vetted not only for their legal acumen but also for their knowledge of analytics and cutting-edge tools.

One trend that is gaining steam as part of the effort to cut the cost of legal services and to improve overall results is the creation dedicated teams of attorneys who are employed by the outsourced provider but who work exclusively for a corporate client. These teams operate effectively as staff attorneys for the corporation — **they are completely familiar with the client's business** and their data, a knowledge base that is built over time. Importantly, they are also skilled at **navigating advanced analytics workflows** to quickly identify key documents and case themes. As such, they can bring that level of experience and skill to each new matter and support the client and their outside counsel throughout the process.

The following are the types of work that they can accomplish:

- **Early Case Assessment**—As discussed above, the outsourced team can provide valuable insights into data at the front end of the case. Familiarity with client specific data can streamline efforts and avoid the challenges associated with unexpected obstacles. Working closely with the corporation and their outside counsel, the outsourced team can explore the appropriate tools that will assist the legal team in achieving their goals and quickly find key information that will likely drive decisions about how to shape the case. An important feature of the ECA process is the identification of data that is either marginally relevant (perhaps requiring only minimal review) or not relevant, thus significantly reducing eDiscovery spend.

- **Document Review Process**—Assuming that there is a need for document review after data interrogation, the knowledge acquired during the ECA process can be leveraged and the dedicated team will be the core group to handle the document review process. For many cases, the core group may be sufficient to handle the

document review phase. To the extent that a larger team is needed, the dedicated team will oversee the work of the first level review team. The dedicated team can also handle some portion of the "second level" review, work that typically would be handled by an outside firm at a much higher cost.

- **Deposition Preparation**—the dedicated team will work closely with outside counsel to assist them in preparing for depositions, for example, by identifying documents that will be germane to particular deponents. In addition to using search terms, this team can use more sophisticated tools to identify interesting and useful content. They can also provide summaries to counsel on the relative significance of those documents for the deponents. Post depositions, the dedicated team can prepare summaries of the depositions for the legal team.
- **Witness Preparation**—the dedicated team can conduct fact research to help the legal team prepare fact witnesses for trial. During the expert phase of the case, they can provide assistance in preparing the experts' initial and rebuttal reports. For the rebuttal reports, they can review any sources of information cited by the opposing party's experts and assess their significance in the case.
- **Trial Prep**—the team can also help to prepare the direct and cross examinations of fact witnesses and assist with the compilation of trial exhibits.
- **Appeal**—the dedicated team can identify key trial testimony and trial exhibits that support the party's arguments on appeal.

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* (2023). Reprinted with permission, © 2023, Thomson Reuters.

A link to the book appears below:
https://store.legal.thomsonreuters.com/law-products/Treatises/eDiscovery-for-Corporate-Counsel-2023-ed/p/106893501

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.

AI Evolution: Prompting and Problem Solving

The world of artificial intelligence (AI) is evolving at rapid speed, especially with the rise of generative AI tools. Large language models (LLMs) like ChatGPT have the potential to automate or expedite any task that requires the recognition and generation of textual content at quality levels that are often indistinguishable from human-generated text. These LLMs are in the early stages, so the output often lacks context and requires human review. This will improve quickly as the model trains with more data.

In the legal industry, the prospective generative AI use cases for both corporate legal departments and law firms are plentiful. The most significant short-term opportunities will likely be optimizing internal processes. Examples include generating reminders around security, compliance, and information summarization across commercial contracts; incorporating generative AI into existing eDiscovery solutions; template creation; and brief drafting.

As with any new technology, the implications of usings LLMs are a top concern in the legal industry. There is a desire for deeper understanding of how this technology works to determine optimal use cases and limit risk. Prompt engineering and problem formulation are two areas to explore further, as these processes are paving the way for better-trained models.

Prompt Engineering

Prompt engineering refers to the process of understanding and refining the questions a user asks an AI or LLM system to get optimal results. The ability to optimize questions lead to better output with minimal amount of back-and-forth prompting. Users have found that merely asking questions without being strategic can lead to generic or incorrect output. Industry leaders in this area are helping to formulate these prompts, which will prove valuable and limit risk in the legal use cases noted earlier.

Best practices have surfaced regarding how to strategically ask questions. This includes prompting the tools to tell the user what else it needs to do a certain task or solve an issue; apply a specific framework to a problem; or act as if it is a person in

a certain profession. Prompts like this help direct LLMs to the right data, output more personalized results, and be refined over time through conversation threading. For example, using the prompt “act as if you are a tutor for the Bar exam” would guide the tool to training data specifically from this area. Having more context allows the bots to generate more tailored responses and lessens the risk of receiving false information.

The quick evolution of AI models leads to less prompting needed over time. This will only continue and allow systems to learn at a faster rate. As advancement occurs, these systems may even be able to craft their own prompts. Linguistical challenges may also arise, as prompt engineering requires a strong focus on the language used to craft questions. Even a small linguistical nuance can alter the output. Some industry professionals believe that the need for prompt engineering is not as significant as first understood because of these reasons. For now, having a partner that is at the forefront of prompt engineering can help organizations use these tools responsibly and open the door for focus on more specialized needs such as problem formulation.

Problem Formulation

Problem formulation is a skill that some analysts believe is the real area of need when it comes to harnessing and training AI systems. This requires getting a firm grasp on the problem needing to be solved in order to pinpoint the right input.

This process differs from prompt engineering, which focuses on the capabilities of a specific tool to determine the best questions to ask.

Along with prompt engineering, problem formulation is a developing area. To hone this skill, several competencies become important. This includes being able to diagnose a problem succinctly, breaking down complex problems, reframing issues, and thinking of the constraints needed to direct an AI system. With complex legal issues, this requires the access to the right expertise and technologies.

Being able to clearly define a problem should allow users to guide these tools better, alleviate linguistical roadblocks inherent in prompting, and maintain creativity and control when formulating a solution. If the problem is clearly defined, then any issues with the language used in a prompt will no longer act as barriers to reaching the solution. This aligns with goals inherent in legal practice – getting clients the best results in the most efficient manner while still maintaining legal judgment over the ultimate solution. It will be interesting to see if and how the "problem formulation approach" trends.

Conclusion

For now, it is important to monitor the developments with both prompt engineering and problem formulation. Even if focusing on the problem becomes more mainstream, prompts will remain a valuable asset to have in order to use AI tools more effectively. These two processes will likely intertwine in the future. Having a partner that is a pioneer in these areas will allow corporate legal departments and law firms to decide on appropriate use cases, be strategic, safely use these tools, and maintain marketability.

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.

Proceed With Caution: Understanding 2023 DOJ Guidance on Ephemeral Messaging

The corporate world has once again been forced to adapt as communication trends change. When ephemeral messaging first gained popularity, it was merely a fun way to send disappearing pictures or messages to friends over apps like Snapchat. Using tools with these capabilities for business communications was unthinkable. Views have shifted as more deploy platforms such as WeChat or WhatsApp for business. This has forced organizations to ponder embracing this new technology, reconsider policies, and explore potential workplace benefits. It is crucial to follow emerging guidance in this area to stay compliant.

Prior Guidance – Sedona

Ephemeral messaging is still a developing topic when it comes to business functions. The Sedona Conference weighed in on the benefits in a 2021 commentary to help regulators, the courts, and organizations navigate ephemeral messaging in business. The conclusion was that it is an acceptable tool but requires caution. For example, it could help with privacy initiatives by safeguarding sensitive data and communications or be useful in a limited fashion with retention management and data minimization.

However, organizations must understand that these tools can bring more risk to the table and therefore should not be used for everyday communications or be central to goal achievement. Using these platforms introduces more risk to govern, such as the failure to preserve information relevant to litigation or an investigation. Information governance updates will also be necessary to notify employees of what data is allowed to be transmitted over these apps.

Several agencies have also expressed that the ability to facilitate criminal activity like fraud or hide relevant information to a case is a serious concern. For years, email has been the preferred method in business. With the rise in chat adoption, the scale of chat usage is now higher than email in most instances. This generally refers to apps like Teams, but some are adding ephemeral messaging platforms to the list of approved communication channels. In this setting, the reduced formality heightens the concern of fraudulent or malicious actions occurring in the workplace.

As such, organizations using ephemeral messaging need to be conscious of how the apps are programmed to delete, what data gets stored, and the types of communications that employees are engaging in on various platforms.

Prior Guidance – The Courts

Ephemeral messaging has started to come up in the courts which will help best practices develop further. For example, judges have concluded that once litigation is on the horizon parties should cease communication over ephemeral messaging platforms. This hinges on when the duty to preserve arises, even if that duty is triggered well before filing suit. In *Fast v. GoDaddy.com LLC*, No. CV-20-01448-PHX-DGC (D. Ariz. Feb. 3, 2022), the court deemed gathering of information and retaining counsel for severance negotiations two years prior to filing suit still triggered the duty to preserve and avoid communications over ephemeral messaging applications.

Organizations should continue to monitor court decisions and utilize these tools in a limited capacity. What is acceptable will look different for everyone and require strategic deployment and clear communications to the entire enterprise about if, when, and how this technology is acceptable in the workplace. The Department of Justice (DOJ) offered some insight earlier this year that could jumpstart more dialogue on the benefits, risks, and best practices related to ephemeral messaging.

Recent DOJ Guidance

The DOJ initially supported a prohibition on ephemeral messaging. Since 2019, the agency has taken a lighter stance indicating that organizations should place appropriate guidance and controls on personal devices and ephemeral messaging in the workplace. All efforts taken to preserve data would be instructive, even when ephemeral messaging platforms were involved. Over the past four years, the DOJ had not provided firm guidance on what this means, which has left organizations unsure of how to remain compliant.

In March, the DOJ finally released long-awaited parameters on how it would evaluate corporate compliance. Key areas highlighted were ephemeral messaging, personal devices, and communication platforms in the workplace.

Here are important takeaways from the updates to the DOJ Criminal Division's Evaluation of Corporate Compliance Programs.

- The DOJ outwardly recognized that it needs to adapt to modern communication preferences and understands that all types of platforms can help organizations grow and communicate more effectively. This includes the use of ephemeral messaging platforms.
- While there are proscribed factors to steer evaluation, the review should be unique to each organization. This provides flexibility to consider business needs, risk appetite, and prior mitigation efforts.
- Prosecutors now have three categories to use for identifying, reporting, investigating, and remediating misconduct and noncompliance with the law. This includes reviewing an organization's electronic communication channels, policy environment, and risk management.
- When evaluating the use of electronic communication channels, examples of what the DOJ will consider include the types of platforms used, what they are used for, limitation imposed on messaging applications and personal devices, efforts deployed to preserve information over each channel, and deletion settings.
- When evaluating the policy environment, examples of what the DOJ will consider include preservation policies, security controls, monitoring efforts, personal device policies, messaging application policies, and governing laws applicable to the conduct at issue.
- When evaluating risk management, examples of what the DOJ will consider include an organization's disciplinary procedures for employee non-compliance, past instances of handing employee non-compliance, and how policies interact with the particular organization's risk appetite.

While the new DOJ guidance provides flexibility for organizations to use ephemeral messaging platforms if they deem it beneficial, it is crucial to keep in mind that communication over such channels may still be subject to disclosure in the event of an investigation. Now that a few months have passed, organizations should be familiar with these updates and continue to assess controls to data retention and preservation.

Conclusion

Based on the guidance to date, what can be done to limit potential fallout? Organizations must think strategically about which communication channels are necessary to conduct business. If ephemeral messaging or personal device usage are on the table, determine which limitations to set in order to alleviate preservation concerns. Have policies in place that are updated as needs change, monitor employee compliance, provide regular trainings, and follow through with consequences in the event of noncompliant behavior. Explore partnerships with providers that can help create robust compliance programs and deploy data-driven assessments to ensure everything is operating as desired. Above all, continue to monitor guidance and enforcement trends from the DOJ, courts, and other agencies as this area of law continues to develop.

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 Down the New SEC Cybersecurity Rules

On July 26, the Securities and Exchange Commission (SEC) adopted new cybersecurity rules. Organizations will need to disclose material cyber incidents pursuant to a prescribed timeline and information regarding risk management, strategy, and governance on an annual basis. The goal is to bring consistency to the disclosure process to benefit both organizations and their investors. Any business registered under the SEC is subject to these updates and should take steps now to comply.

New Requirements

The new SEC rules will require process reevaluation and changes. Leadership teams and legal departments must work together to make updates and maintain adherence to the new standards. Here is an overview of the key additions:

- When a material cybersecurity incident occurs, organizations need to disclose it on Form 8-K within four days after deeming it material. The disclosure must include the material nature, scope, timing, and impact of the breach. There is a narrow exception to the four-day rule if the U.S. Attorney General determines that disclosure would be a substantial risk to national security or public safety.
- In the annual report on Form 10-K, organizations now must include three new categories of information. The first is all active processes for assessing, identifying, and managing material risks from cybersecurity threats. The second is any material effects of risks from cybersecurity threats and prior incidents. The last is a description of the board of directors' oversight of cybersecurity risks stemming from threats and management's role and expertise in assessing and managing material cyber risk from these threats.
- Foreign private issuers will also need to provide the same disclosures listed above on Form 6-K for incident data and Form 20-F for risk management, strategy, and governance efforts.
- The rules go into effect 30 days following publication in the Federal Register. Public companies will be required to comply with new form disclosures for cyber incidents starting Dec. 18, 2023. Smaller reporting companies have a longer grace period until June 15, 2024. To be considered smaller, a company must fall within one of the following categories: The first applies to those with less than $250 million of public float. The second applies to those with less than $100 million in annual revenues and either no public float or a public float less than $700 million. The risk management, strategy, and governance disclosures need to be included in an organization's first annual report for fiscal years ending on Dec. 15, 2023 or thereafter.

Public Reaction

On initial release, the four-day rule has caused some concern over how early in the process this is, as remediation will likely still be occurring. Anticipated obstacles include meeting the tight timeline, not having the full picture of what data was breached and who to notify, correctly labeling breaches as material, and lack of clarity over whether this would obviate the need for individual notice. There may be some hesitancy or confusion on when to report cyber incidents, incomplete reporting from not having enough information available, and concern over false reporting an event. Current best practice runs counter to the new rule's approach. It guides that there should be no reporting until absolutely sure a breach occurred and it is stopped. Also, that the organization understands the scope and that reporting facts prematurely or inaccurately exposes them to other types of risks and repercussions. The

incident rule also applies to breaches involving third-party providers. Having a trusted relationship with providers needs to be prioritized, as does having a mature process for vetting and approving providers. This should include assessment of their cyber posture and preparedness.

The SEC made changes in the final version of the rules to address some of these worries, including not requiring disclosure of technical details for a breach. Also, by leaving room for judgement on what is considered material and when the four-day timer begins. This is fact-dependent. There will be more clarity on how the SEC addresses remaining questions once reporting begins. Taking steps to comply beforehand will place an organization in the best position to respond quickly, while also creating a better culture of cybersecurity management and governance.

Compliance Tips

All organizations should strive to develop good cyber hygiene. As the threat landscape evolves and new tools trend, the compliance standard will also change. The new SEC rules underscore the serious threat cyber incidents pose and how to respond in a uniform expedient manner. This is a C-suite level initiative and there needs to be board-level attention on minimizing, managing, and responding to cyber risk. This can be accomplished by having a robust cyber incident preparedness and response plan. For those organizations who already have one in place, it is time to review and update it to comply with the new rules. Legal should also be a key player in this process.

Many organizations and legal departments will need to get up to speed on understanding the requirements for their incident response plans and remediation process. Grasping the steps and time involved in responding to an actual event is crucial. The focus should be on ways to improve preparedness such as having regular tabletop exercises, employee training on how to report suspected breaches, designated incident contacts, escalation processes, tools to monitor attack trends and security vulnerabilities, and increased involvement by the C-suite. All of this will help organizations pinpoint potential threats so they can take appropriate steps to limit risk, manage information better, and respond to incidents quickly – all while remaining compliant.

Having a relationship with a provider that can offer both proactive planning and response efforts is a game changer. This will ensure that the C-suite, legal, and other important actors are aligned on cybersecurity initiatives and ready to respond in the event of a breach. Since breaches involving third-party provider systems also need to be reported, having a longstanding partnership will allow for more seamless communication to aid with fulfilling reporting requirements. On annual reports, organizations will also need to include information about providers and consultants that assist with cybersecurity planning and response programs.

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 Governance vs. Information Governance-Know the Difference

Data governance and information governance may sound like interchangeable terms, but they are not. Both have unique histories and have evolved over time, but they also overlap in several ways. In the evolving digital landscape, it is crucial to identify how these processes differ and complement one another. While it is true these are two separate disciplines, with the proper strategies in place they work together in perfect synergy. Investing in both areas and creating workflows allowing these processes to intertwine can benefit business in several areas. This includes improvement to data quality, compliance, risk management, and decision-making.

Distinctions

A simple way to distinguish the two disciplines is through a LEGO metaphor. Data governance represents the individual LEGO pieces while information governance incorporates the sorting, arrangement, and creative structures that can be built using those pieces. To better understand the distinctions, let's look at how each has evolved over time.

Data governance has a longer history going back to the 1960s. It involves the processes and technologies used to organize, store, and protect data assets within an organization. It is primarily focused on ensuring data accuracy, accessibility, and availability. The explosion of data, increase in data breaches, and expanded privacy laws around the globe have shifted this practice. Organizations are now increasing their focus on improving the mechanisms used to manage and secure their data. The availability of data analytics and business intelligence tools has also added to the value of having quality data.

Information governance began in the early 2000s due to increased focus on electronic records in the discovery phase of litigation. It encompasses the policies, processes, and controls that enable organizations to manage their information assets effectively. This practice broadens data governance by addressing legal, regulatory, and compliance requirements while additionally aligning information with business objectives. Information governance has shifted over time due to new tools available to manage data, the expanded use of AI for business processes, and ever-evolving legal and regulatory landscapes.

Data and Information Governance Working Together

While data governance focuses mostly on the technical aspects of data handling, information governance takes a broader approach by incorporating legal, regulatory, and strategic considerations. Both are vital for maintaining data integrity and leveraging information as a valuable asset. These two practices are truly complementary in nature.

Take data privacy management for example. One of the biggest challenges many organizations face today is carrying out their data privacy initiatives, as the landscape is evolving at a fast pace. There are several differing laws that may apply to an organization's data handling and create new compliance obligations, including information that requires extra safeguards. The role of data governance could come into play here through data mapping, storage methods, new security features, and tailored metrics relating to privacy. The role of information governance could apply when consider the differing legal and regulatory data privacy landscapes applicable to an organization's activities. Then, creating strategies around compliance such as new policies for data retention and risk management tools.

Having a partner that can advise on privacy processes and best practices is key. This includes access to technology for

implementing, customizing, building, running, monitoring, and enhancing data privacy risk management initiatives – and the expertise behind the tech to tie it all together.

Benefits

Having a comprehensive understanding of data governance and information governance can provide meaningful support. By implementing robust data governance and information governance practices, organizations can reap several benefits. They can enhance data quality, mitigate legal and compliance risks, and unlock the full value of their information assets. This ultimately leads to better decision-making and improved business outcomes. Failure on these fronts carries several risks including missed deadlines, unfulfilled legal or regulatory obligations resulting in fines, reputational harm, dissatisfied clients, interrupted business activities, and other liabilities.

In a report from Data Ideology, 78 percent of businesses that implemented robust data management strategies reported improved decision-making processes and enhanced data-driven insights, propelling them ahead of competitors. Industry analysts also forecast significant growth to continue with cloud-based information governance in response to several factors such as data privacy obligations, the need for tighter security, and ever-increasing amount of digital data. All of this illustrates the growing importance of investing in both areas and having the right support to choose optimal tools that support governing initiatives.

Conclusion

The market for governing data and information is booming and will continue to grow into the future. Organizations that manage their data and information effectively will have a competitive advantage as new data and information privacy laws are passed in legislatures, and as tighter records retention regulations are implemented. Also, with the rapid rise of generative AI, the quality of data and information will be critical to realizing opportunities to use AI to improve client services, research, and lower costs. Creating strategies around harmonizing both processes will be the key to 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.

Changes in Legal Operations – A Look Back Over the Last Decade

As the legal landscape evolves at unprecedented speed, the role of legal operations within a business continues to transform. Legal departments are under increasing pressure to serve the business and reduce costs. This looks different for every organization and needs change as priorities shift, outside factors influence business demands, and new technology trends. When the concept of legal operations first emerged, it was broadly defined as finding ways to run legal more like a business. This characterization still rings true today, but as the industry develops so do the roles of legal operations professionals. There are more defined responsibilities that fall under this umbrella and connect legal with the entire enterprise.

The Evolution

Ten years ago, the role of legal operations was akin to a general counsel's chief of staff. Some even have a legal chief of staff or a hybrid chief of staff/head of legal operations title. For many the role was more administrative encompassing tasks such as billing management, meeting preparation, vendor management, technology planning, policy review, and process improvement. As the role evolved, more professionals also started acting as a liaison between the general counsel and other parts of the business to facilitate better communication and drive decisions.

Over the last decade, professional organizations dedicated to bringing the legal operations community together have grown. The desire to explore innovative approaches for running legal like a business has also deepened. This has sparked change in the industry to make the role of legal operations a more strategic one. The wide the range of business processes and activities that can help legal departments run more efficiently is increasingly apparent. More organizations of all sizes have brought legal operations professionals in-house and created specific roles dedicated to this function or refocused the role away from the administrative side.

There are also opportunities to partner with outside consultants that assist legal departments with meeting near-term challenges and planning for a digital, technology-enabled future. Overall, the legal operations function is critical in harmonizing enterprise level goals with legal service delivery.

Importance of the Changing Role of Legal Operations

Investing in people that can help effectuate meaningful change and drive strategic initiatives for the legal department is key. This requires a deep understanding of why legal operations is an important function and the value that strategy-focused individuals can bring to the plate. Here are four reasons to consider.

1. **Legal operations professionals act as strategic partners that can bridge gaps between legal and the business.** Having an in-house legal operations team or outside consultant that focus on solutions demonstrating value to the business is truly transformative. Legal departments can achieve performance excellence via tailored comprehensive strategy, technology, and change management initiatives. Trending areas that legal operations teams are targeting include contract management, knowledge management, technology and vendor vetting, regulatory compliance, metrics, legal spend, and outside counsel management. Aligning these functions with business goals leads to better risk control, cost efficiency, and enterprise-wide collaboration.

In many of these areas, the legal operations role has shifted. For example, some professionals have a seat at the decision-making table and make buying decisions for the department. This has moved beyond being a communication liaison for the general counsel to having a voice in why certain investments are worth keeping in or out of the budget, the most efficient way to get there, and how it all ties to enterprise-level goals.

2. **Legal operations professionals help navigate tech innovation.** Legal operations teams can advise on ways to leverage tools that help meet strategic goals, which will look different for every organization and change as new priorities emerge. With new legal tech solutions constantly entering the market, appropriately scaling technology and justifying investment to the business can be a tough task. Legal operations professionals have the experience and resources to not only manage and track performance for legal tech investments, but also change company culture when it comes to embracing new solutions. Through design thinking, these teams can pinpoint ways to streamline processes that create efficiencies and reduce bottlenecks while also considering new ways to deliver services.

3. **Legal operations professionals use data to formulate creative solutions.** Having advanced metrics and data analysis capabilities to guide strategic decisions is a proven game changer. General counsel should look for partners that can empower legal teams to re-envision the delivery of legal services, create necessary and data-driven strategies, and then execute new plans successfully. A solid approach includes benchmarking against internal and industry data, creating a roadmap, and then delivering results. Having metrics and access to legal business intelligence is a tangible way to illustrate industry trends and demonstrate legal's value to company leaders.

4. **Legal operations professionals can formulate roadmaps for the efficient, cost-effective, and compliant delivery of legal services.** Many larger organizations are now creating legal panels that consist of pre-approved outside counsel. This helps streamline case assignments, instills predictability, and provides reassurance that the right lawyers will be available to tackle complex and varied issues. Legal operations professionals have the skillsets to set criteria for these panels, which encompasses thorough consideration of the legal department's needs and budget. They can also implement adherence to outside counsel guidelines.

Conclusion

So, what will the next decade look like for the legal operations industry? One thing for sure is that it will keep growing and become even more integrated in the role of delivering legal services. The reasons why legal operations professionals are important to an organization will continue to lengthen, but the underlying theme will always be that they can connect legal with the rest of the enterprise. There is no doubt that this will continue to evolve into an even more strategic role.

The business world is in an extremely dynamic and transformative period, with innovation soaring and technology driving new ways to get work done. Legal operations is the link to help general counsel build a culture of compliance, optimize workflows in every department, manage costs, and navigate changes that surface.

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.

Effectively Creating and Managing a Data-Driven Compliance Program

The regulatory landscape is drastically changing. Increased regulator intervention and oversight, new laws, and globalization makes it tough to stay on top of compliance obligations. Duties generally arise under law – such as data privacy or financial regulations – or during litigation and investigations. The long list of potential compliance drivers and evolving data sources has created a noticeable shift where more organizations are prioritizing compliance initiatives.

Deploying targeted processes and solutions is the way to stay afloat. The industry has started to explore whether artificial intelligence (AI) can provide a reasonable programmatic response.

Shifting Historical Practices

Most organizations likely have already implemented some type of compliance workflows, policy guidelines, and training. Having a comprehensive program considering both proactive and reactionary measures has not been the norm. For organizations operating on an enterprise scale in several locations, there is even more information to manage. When a compliance requirement arises, an organization may be required to share information at a moment's notice. Additionally, several regulators are broadening investigatory powers, placing higher scrutiny on settlements, and even requiring robust compliance programs. All of this means that providing compliance training and baseline reactionary programs are no longer enough.

Organizations need to implement proactive monitoring and prevention strategies. Government agencies, corporations and their counsel are now creating and implementing compliance programs to track a wide range of corporate conduct in order to stay ahead of the curve. An emerging best practice is to deploy a defensible compliance program that can be integrated with existing tech and has enforcement capabilities. Working with a consultant that has the right knowledge, expertise, and tools can help overcome cost impediments and create tailored plans aligning with their requirements.

Turning to Data

Now that organizations are reimagining their compliance programs, the question becomes: what tools are best suited for the job? This developing area of the law lends itself naturally to AI-based technology solutions that are guided by legal counsel. Industry professionals are currently debating whether AI is the magic bullet and how to use this technology to maintain a successful data-driven compliance program.

Here are key considerations to keep in mind when undertaking this feat:

- The use of AI for compliance will likely start trending but will be looked at closer until it becomes more mainstream. Having a provider partner that can demonstrate that these tools are superior to previous methods can help alleviate this burden. The ability to proactively monitor and pinpoint behavior before a compliance issue arises will be a driver here.
- To provide adequate compliance, a program also needs to address governance and security challenges faced by today's law firms and corporate legal teams. Having these two areas in order will lead to smoother compliance activities when the time comes. Data mapping, carefully crafted retention policies, and implementing extra

security measures are a few areas to explore. This also requires collaboration between legal, IT, and other business teams to understand how certain datasets can inform compliance issues and where to access this information.

- Tapping into data from eDiscovery tools can help teams use problems of the past to inform the future. This includes pinpointing behaviors that gave rise to litigation in the past. Portable AI models are one option to explore.
- Discuss additional legal and ethical implications for using AI solutions to track behavior. This includes the potential of creating a data depository that can be subject to discovery requests, privacy considerations, and protecting information subject to attorney-client privilege.
- Understand what different regulators are looking for to deem a compliance program sufficient. If the program is well-designed, applied in good faith, and proven successful in practice then it is likely that the burden will be filled.

Considering the points noted above will help organizations stay ahead of the curve when updating their compliance programs. Spending time on improving internal collaboration, security, and information governance will lay a solid foundation to make this a reality. Having a provider partner that can harmonize these efforts and bring in new technologies, including AI for compliance, will also prove beneficial as this area evolves.

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 Remain Data Defensible During Divestitures

Create a divesture strategy, monitor the portfolio, find a buyer, prepare to separate a portion of the business, close the sale, and oversee the transitionary period. This is the usual flow of events during a divestiture, but one key component cannot be discounted during this process – defensible data segregation. Before getting into why this is a key element of divestitures, let's break down what it is and why an organization may decide to divest.

A divestiture is when a company sells, exchanges, closes down, or otherwise disposes of part of their operations. This is generally a strategic decision to maintain profits when a certain business unit is not performing as well, is no longer relevant to their core competencies, or becomes redundant due to M&A activity. However, divestitures may also result from bankruptcy proceedings as a way to meet outstanding debts and reorganize the company.

When divesting assets, it is crucial not to forget what information is contained in the data being sold to avoid any legal, regulatory, or contractual violations. Here are two steps organizations should add to their divestiture checklist that can help identify and segregate confidential data defensibly and remain compliant during the process.

1. Don't Forget the Information Governance Component

When going through a divestiture, the sale will include company data but this does not mean that all the data from that business line should migrate over to the buyer. It is critical to identify and review information prior to migration to avoid disclosure of data that could open the divesting organization up to liability. Advancing defensible information governance processes to identify and segregate data is key and an important part of risk management efforts.

There are several reasons to have a defensible data strategy. This includes avoiding disclosure of information that would violate a law or regulation, such as privacy obligations. Organizations will also have clauses protecting confidential information in their contracts, settlement agreements, and other legal documents. Lastly, there may be proprietary

information and trade secrets comingled internally that could be accidentally divulged during a divestiture if the organization fails to perform due diligence or establish strong information governance procedures.

A data-driven information governance strategy will not only help safeguard sensitive data, but also establish ownership, limit the risk of breached information during transfer, and keep operations running smoothly. This can be tough with larger organizations that do not have their data in order, as information inevitably becomes comingled. Facing divestiture deadlines on top of this can render it hard to efficiently transfer the right information out, maintain ownership over the data that needs to remain with the divesting company, and effectively close down a business line. This is where outside expertise is valuable.

2. Seek Help From the Experts

A partner with the resources to implement robust information governance and data security practices that has divestiture experience is the key to a smooth transaction. A provider can help organizations get their houses in order as a proactive measure. Having clear retention and storage policies, data mapping, records management tools, and segregated systems are solid options to explore.

Once the divestiture process begins, that partnership will already be established to tap into quickly. Approaching data segregation in the following manner can reduce the risk

of exposing trade secrets or other confidential information during the process.

1. Apply exclusions to confidential and sensitive data types
2. Identify inclusionary data related to the divested entity
3. Review all necessary data in place prior to migration

A provider that understands the organization's systems and information governance practices can implement these steps and segregate data more efficiently. Another plus is when the data can remain in the organization's systems whether it lives in the cloud or on-prem. This eliminates additional costs for searching, analyzing, and reviewing data.

For example, many organizations use Microsoft products to chat with colleagues, hold meetings, create documents, and much more. There is a high chance data that needs to be segregated prior to divestiture will live in this environment. Having a provider that can leverage a tool such as Microsoft Purview will help fulfill divestiture requirements without incurring any external storage fees and keep all sensitive data within their internal Microsoft system. This is a prime example of how having the right external advisors with expertise and access to the right tech can make all the difference.

Conclusion

Before moving forward with a divestiture, organizations should be thinking about their data. Failing to be thorough risks disclosure of confidential information. This can lead to unhappy clients, legal liability, data breaches, operational interruption, and reputational harm. Prioritizing information governance and collaborating with outside expertise will foster effective transactions and keep data where it needs to live. Having the same provider to turn to not only for a divestiture but for long-term information governance strategies will ensure that organizations are handling their data in the most efficient and risk-conscious manner.

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.

A Look Into 2023: What do the Bankruptcy Statistics Really Mean?

It has been quite the interesting year in bankruptcy so far, with filings increasing in several chapters. Providing some market observations based upon the number of filings for commercial and consumer bankruptcy filings can assist professionals in aligning their practice focus for the remainder of 2023. This requires an understanding of the current economic conditions, debt maturity dilemma, and how bankruptcy fits into the picture.

The Bankruptcy Data

Data collected by Epiq Bankruptcy provides state of the market observations, highlighting commercial and consumer bankruptcy filing trends. This data shows that the numbers are up across the board.

- Total bankruptcy filings were 217,420 during the first half of 2023, demonstrating a 17% increase from the 185,352 total filings during the first half of 2022.
- Getting more granular, total commercial filings were up 18% from last year and individual filings were up 17%.
- Chapter 11 commercial filings totaled 2,973 during the first half of 2023, which was a 68% increase compared to the first half of 2022.
- Small business filings, which are identified as Subchapter V elections of Chapter 11, totaled 814 in the first six months of 2023, demonstrating a 55% increase compared to the first half of 2022.
- Chapter 13 individual filings totaled 85,390 during first half of 2023, which was a 23% increase compared to the first half of 2022.
- All chapter filings increased in June 2023 compared to June 2022, with 37,700 total bankruptcy filings representing a 17% increase. Looking at June comparisons, commercial filings were up 12 percent and individual filings were up 18 percent.

The spike in bankruptcy filings may be puzzling as the economy seems fairly stable given the positive employment rate and the Federal Reserve's attempts to curb inflation have had success.

Uncertain Economy

This year there has been unforeseen turbulence in the market coupled with uncertainty. What is different from the conditions last year is that the forecasted turbulence in 2022 was expected due to pandemic-related events. The comprehensive federal relief during the height of the pandemic brought relief to both corporations and individuals. The economy was clearly impacted by the blanket shutdown but 2023 has seen a rebound with higher employment rates, stable or increased home values, and supply chain relief.

However, many observers believe a recession is looming due to the massive debt accumulation during the pandemic. The economy is seemingly stabilized, but the enormous amount of outstanding corporate debt with upcoming maturities cannot be ignored. Given the debt maturity wall is looming, organizations may face significant challenges raising money in this interest rate high environment. There is also uncertainty in several industry sectors such as cryptocurrency, commercial real estate, and retail. The effect of student loan repayment could increase individuals filing nationwide.

Predictions

It is truly an unprecedented and interesting time in bankruptcy. Observers are not clear on where the economy is headed. Chapter 11 filings are on the rise, but not nearly where the restructuring industry envisioned given the effect of the pandemic on corporate performance. What will happen going forward? Below are five predictions and areas to monitor the remainder of 2023 and beyond.

1. An increase in Chapter 11 filings will continue into the near future. While many challenges have eased, the rate of inflation and increasing interest rates are impacting corporate action. As the cost of money increases, servicing debt will prove difficult and may warrant bankruptcy protection. The increase in Chapter 11 filings indicates that companies – predominantly middle market – are unable to fund their businesses and service their debt.

2. There will be more Subchapter V filings. Subchapter V provides a simpler, expedited, and less expensive way for qualifying small businesses to restructure their debts. The debtor can enter a repayment plan to pay creditors in exchange for retaining equity ownership in the company, providing continued viability for the struggling business. The increased eligibility limits for Subchapter V elections are currently set to sunset on June 21, 2024. The American Bankruptcy Institute has formed a task force to study small business reorganizations and issue a report of observations and recommendations to be released in April 2024.

3. The economy will remain disconnected for a while. Put simply, money is too expensive to borrow right now so there is little room for strategic growth. There has been rising inflation, tighter lending restrictions, and much higher interest rates. For a decade prior to the pandemic, rates were at historical lows. With these higher interest rates, companies facing liquidity challenges will be unable to secure adequate financing and will continue to struggle. As such, Chapter 11 has become a more useful tool as companies need to address their debt-ladened capital structure.

4. Student loan repayment will continue to be an uphill battle. Repayment compliance of student loans have been in a state of uncertainty over the past several years. While it may not rise to the level of an economic bubble, there is approximately $1.77 trillion of student loan debt outstanding. While no one can predict the ramifications of non-payment, one thing for certain is that it will affect the economy negatively. The current administrative relief programs may provide some relief but may not be sufficient to prevent borrowers from filing individual bankruptcy.

5. Several factors will continue to influence individual filing trends. According to USA Today, medical debt has contributed to about 66.5% of bankruptcies. This will persist, especially since medical costs have been increasing with inflation. Another factor to consider is affordable housing. Obtaining or refinancing a mortgage in this higher interest rate environment could lead to more bankruptcy filings. It's interesting to note that foreclosures have been at an all-time low due to moratoriums, but that clearly cannot last. Finally, as more businesses feel the effects of managing larger debt thresholds, layoffs are inevitable which in turn will likely increase individual bankruptcy filings.

Guidance

Based on the current trends in the economy and the escalating bankruptcy numbers, bankruptcy professionals should brace for more filings across all chapters. This trend is evidenced by the spike in the number of filings as there will undoubtedly be a similar wave in the second half of this year as organizations consider their options to pay off outstanding debts.

Above all, having the right resources, expertise, tools, and partnerships in place to navigate the current landscape is needed. Now more than ever it is crucial to monitor lending trends and the overall state of the capital markets which can provide insight into the best strategies to stabilize businesses.

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.

Move it or Lose it – With Cyber Breach Response, Time is of the Essence

There are so many factors that go into breach response. Determining the size of the breach, time limitations, legal requirements, notification needs, urgency for containment, and interrupted business operations are just a few. Once a cyber security incident results in a data breach, reaching those affected needs to be done quickly, thoroughly, precisely, and reliably. Oftentimes large-scale outreach to large groups in short windows of time is necessary to maintain proper compliance and limit liability exposure.

In addition to internal breach risks, organizations cannot discount the potential for an outside event to enter their environments and wreak havoc. Certain events can cause widespread attacks that quickly place a large number of organizations at risk. A prime example is the MOVEit hack that began in May 2023 that many are still reeling from. Understanding the effects that widespread hacks can cause and the best resources to tap into if one occurs is critical. Let's digest the MOVEit breach as an illustration.

The MOVEit Breach

What happened with MOVEit is an example of how a small vulnerability can quickly turn into a disaster that highly increases litigation exposure. This accredited transfer file management program developed by Progress Software experienced a devastating breach. Many organizations used it for sensitive data transfers, as it met high regulatory standards. A zero-day vulnerability in both the on-prem and cloud environments emerged that no one was equipped to handle. Threat actors were able to gain access to customer accounts. There was no immediate patch available, rendering containment and mitigation extremely difficult. More vulnerabilities have also sprung up along the way.

The hack was traced back to Clop, a ransomware cybercriminal group. According to Reuters, as of August 2023 over 600 organizations globally experienced a compromise stemming from this hack. The article proclaimed, "the sheer variety of victims of the MOVEit compromise, from New York public school students to Louisiana drivers to California retirees, have made it one of the most visible examples of how a single flaw in an obscure piece of software can trigger a global privacy disaster."

Exposure is not limited to organizations that use MOVEit but extends to third-party vendor data. Many incidents involve more than one million affected contacts. Threat actors will continue to trickle out impacts utilizing the vast amounts of data they have exfiltrated. The types of data impacted tend to be rich files with contact data, such as complete client or employee lists containing full PII sets.

Breach Response Efforts

When falling victim to a widespread attack like MOVEit, time is precious. Organizations need expert resources to lean on and limit the fallout. This is where having a cyber incident response partner that can quickly launch a customizable multi-faceted breach response program is a game changer. With such sensitive information at risk, anything that can be done to remediate faster will make a huge difference in how much liability exposure the organization ultimately experiences.

If protected data is exfiltrated or accessed from compromised MOVEit environments, accurate and effective review is essential to create clean lists of affected contacts. This includes employees and customers requiring notification. Timely notification, quality care, and support of these contacts is essential. This minimizes damage, protects brand trust, and helps avoid regulatory fines. Providers offering a breadth of services when opportunistic events such as MOVEit occur can be valuable to limit litigation risk. Look for expertise in data

mining, review, project management, notification, call centers, and credit monitoring.

In the MOVEit breach response landscape – or for any similar event in the future – so much is unknown. The end is not certain with such involved hacks, so it is prudent to have a plan in place for ongoing management. This also provides insight into handling vendor relationships going forward. As the MOVEit breach demonstrated, organizations are dependent on the security habits of their vendors and other third parties. Before partnering with someone, investing in new technologies, or otherwise transferring sensitive data – it is crucial to advance a thorough vetting process to understand all cyber risks.

Conclusion

Widespread hacks exploiting zero-day vulnerabilities are just another thing to account for with breach response. Cyber incidents can be unpredictable, so investing in preparedness efforts is important. Already having a breach response provider capable of delivering services efficiently and at a large scale prior to a devastating event can make a world's difference. This can help navigate the unknown, quickly reach cost-effective resolutions, manage the risk of lost business, avoid steep regulatory fines, and maintain an ongoing breach management plan when needed.

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 Does India's New Law Fit into the Global Data Privacy Landscape?

Changes to India data privacy laws have been a long time coming. A 2017 Supreme Court decision sparked legislative overhaul when concluding that privacy is a fundamental right. A bill was introduced soon thereafter leading to years of review, multiple versions, and debate. In August, India's Digital Personal Data Protection Act of 2023 (DPDPA) received presidential assent. The law was modeled after the EU's General Data Protection Regulation (GDPR). It was originally poised to be stricter than the GDPR but that did not come into fruition, as the final version of the law was scaled back.

Positioned as one of the largest open internet markets and a major hub for offshore outsourcing projects, the India law will likely make a lot of waves and significantly influence global policy. Those coming under the DPDPA's purview need to understand compliance obligations quickly, as it is anticipated to become effective next summer. A firm date is yet to be set.

Overview

Here are ten key provisions to help organizations get started on their compliance journey.

1. Collection and processing activities of Indian residents applies to both organizations located in-country and those in other countries that offer goods and services to India data subjects. Consumers have the typical rights seen in other laws including the right to know, access, correct, and erase.

2. There are no separate provisions applying to sensitive data processing. This is different from the GDPR and some state laws in the U.S., such as Utah.

3. There are no extra requirements for international data transfers with the exception of a few restricted countries. The central government will release a list of these countries. Other laws like GDPR make it harder by requiring adequacy decisions, transfer impact assessments, or contractual clauses for cross-border activity.

4. There are limited exceptions including publicly available data, merger-related transfers, and restructuring transfers.

5. Organizations need explicit consent before processing data, which is a unique feature as other laws like GDPR offer several options. Users can withdraw consent whenever they desire. There are narrow exceptions, including processing for medical emergencies and employment purposes.

6. Organizations must implement reasonable security safeguards to prevent personal data breaches.

7. Data fiduciaries must designate and publish contact information for a data protection officer that can address any questions or concerns about processing activities.

8. An organization may receive a significant data fiduciary designation that carries more obligations. Factors for making this determination include volume of data processed, sensitive nature, security, public order, risk to electoral democracy, and more. Significant data fiduciaries must appoint an India-based data protection officer and independent data auditor. They also must conduct assessments at regular intervals.

9. The new enforcement authority will be the Data Protection Board of India. Duties include mitigation oversight, consumer complaint handling, and investigations. Monetary penalties for noncompliance can reach up to the equivalent of $30 million USD per violation.

10. After a data fiduciary gets fined two or more times, the Data Protection Board can advise blocking access to information in their systems.

This is just a snapshot of responsibilities and as always, organizations must review the law in full to understand all compliance obligations. The central government also plans to release supplemental rules that will provide further guidance and provide a better grasp on the DPDPA's reach.

Compliance Tips

The growing global privacy landscape creates new and sometimes conflicting responsibilities. When more obligations arise, it is crucial to know where overlap and divergences exist in order to maintain a compliance program that meets the requirements of all applicable laws. For those organizations subject to India's new legislation that already have GDPR-centered programs, there will be a fair amount of overlap making the transition smoother. However, as demonstrated above, there are significant differences with India consumer data handling to consider. A provider with data privacy expertise that can implement information management tools, detect security shortcomings, and orchestrate thorough compliance plans is a beneficial resource to help internal teams.

For now, to be best prepared it is imperative to review data collection and processing practices to identify anything that is not up to par with the new law. After identifying deficiencies, organizations can explore ways to bolster security, policies, and notice efforts. A big focus should be on addressing ways to receive adequate consent from data subjects, as this is a major feature of the law differing from other global directives. If and until the central government issues rules clarifying this provision, most processing activities will require explicit consent. Other areas to monitor for further guidance include how an organization's India outsourcing activities creates new obligations and rights, how significant data fiduciary designations unfold, and enforcement trends.

Challenges

Also keep in mind that each law not only brings its own set of compliance obligations, but also challenges. The India law provides a lower bar for international transfers which could affect where companies based in the US or other countries with a less defined privacy landscape decide to conduct business activities. In China, there is a large focus on national security which makes it difficult for international organizations dealing with confidential client data to conduct routine business operations. For example, a law firm may be required to disclose client data to the government or be blocked from transferring data to employees situated in other office locations.

These are just a few examples of the nuanced challenges organizations need to account for when setting compliance objectives and making strategic business decisions. The overall takeaways? Knowing the laws, partnering with experts to guide compliance, and understanding unique obstacles each law presents will help navigate the ever-changing global privacy landscape.

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.

Trending eDiscovery Topics in the Courts

It is crucial for litigators and eDiscovery consultants to monitor case law developments, especially in relation to emerging technologies and changes to legal practice. With the first half of 2023 in the books, it is an ideal time to review hot issues. This knowledge can help litigators anticipate what to expect in court, guide technology and provider partnership needs, and efficiently navigate litigation.

Below are two discovery trends that have continued to grow.

#1: There is an increasing demand for carefully crafted ESI protocols.

More litigators are creating protocols to guide eDiscovery in their cases. Unsurprisingly, this topic has gained momentum in the courts over recent years. Since parties agree to what is in a protocol, most judges follow those directives and allow it to govern the outcome of discovery disputes.

Case law in this area has covered a variety of issues, but the underlying theme is that litigators need to think through what they are agreeing to before creating an ESI protocol. By considering potential issues and bringing disputes to the court at an earlier stage, parties have more clarity going into the process and avoid extra costs and delay. Also, limiting what is in the protocol to account for unknowns and leaving room to amend is emerging as an industry best practice.

Here are two cases from 2023 that illustrate and expand upon this theme:

- In *SinglePoint Direct Solar LLC v. Solar Integrated Roofing Corp.,* No. CV-21-01076-PHX-JAT (D. Ariz. March 21, 2023), plaintiff objected to search terms defendant submitted several times and claimed that a good majority of the production sought from defendant was unnecessary. The parties had agreed to ESI protocols prior without asking the court to review. The protocol did not set a time limit to object.

  While the judge sided with defendant on the proportionality argument, he made it a point to label the protocol as poorly crafted and did not agree with defendant's claim that the objections were untimely. He proclaimed that had they submitted the protocols for approval the court would have deemed them unmanageable, which would have allowed the parties to add in objection timelines and make other necessary changes before moving forward with the case. This illustrates that judges use protocols to guide rulings, want them to be more specific, and see benefit in having the court review them before finalization.

- *McCormick & Co. v. Ryder Integrated Logistics, Inc.,* No. JKB-22-0115 (D. Md. March 08, 2023) is another instance of courts closely following ESI protocol language. A custodian in the case had ceased employment at plaintiff company and all data was deleted. Plaintiff had to retrieve information from six other sources to capture relevant communications and searched the name of the custodian in the ESI already gathered. This greatly increased the amount of potentially relevant documents and plaintiff argued that being forced to review these search results prior to production was not proportional.

  The ESI protocol had a section labeled "no presumption of responsiveness" that said to fulfill discovery production obligations, a party needed to review documents that are potentially relevant pursuant to the methods outlined in the protocol. It went on to state that when a document is captured by a search pursuant to the protocol, that does not necessarily mean it is responsive and some

data will be appropriate to exclude from production. Plaintiff argued that the protocol did not require manual document review pre-production after identifying potentially relevant documents via search terms. The court disagreed, concluding that Plaintiff was not looking at the protocol as a whole as the plain language mandated manual review of documents captured via search terms before production. The judge also found the cost and time burden to be proportional. This ruling is key because had the protocol been more limited, the court may have deemed the tech-enabled review sufficient on its own.

While ESI protocols are not new, these cases show how important they are becoming in litigation. Judges are allowing protocols to guide most disputes and weighing in more often about how or when they should be drafted in order to avoid extra costs and delays. Some analysts predict that data security and privacy obligations may be required in future protocols, so litigators should monitor new case law to see if this occurs.

#2: Judges are still relying on inherent authority to justify sanctions.

Federal Rule of Civil Procedure 37(e) provides a basis for judges to award sanctions when a party fails to preserve or destroys evidence. It has almost been a decade since Rule 37(e) amendments became effective, which intended to streamline sanctions and provides factors that promote consistency. Although these amendments aimed to foreclose reliance on inherent authority, judges are still using it to justify sanctions.

The question persists – should judges be allowed to rely on inherent authority? Legal analysts along with case law suggest the answer to this question is yes, and there have already been decisions involving inherent authority this year. While Rule 37(e) applies in many situations, judges are still relying on inherent authority to issue sanctions where anomalies are present in an effort to reach justice. Judges have continued to use inherent authority both as an alternate to the powers bestowed in the federal rules or in conjunction with the Rule 37(e) factors. This is a very subjective area of the law, as sanctions are dependent on the facts of the case and require an analysis into intent behind the behavior.

For example, in the patent infringement case of Site 2020 Inc. v. Superior Traffic Servs., LLC, No. CV 21-63-M-DLC-KLD (D. Mont. Mar. 27, 2023), the court issued severe sanctions for plaintiff's discovery misconduct. The parties were competitors in the traffic signal industry. Plaintiff had someone attend a business demonstration between defendant and a third-party by posing as an employee of the third-party. The individual secretly recorded the meeting where attendees discussed sensitive information.

The judge proclaimed that in addition to being able to issue sanctions for bad faith actions, the court also has inherent authority to issue case-terminating sanctions when the conduct is deliberate, deceptive, and interferes with judicial integrity. As such, the judge granted Defendant's motion for dismissal sanctions finding that this behavior during active litigation sidestepped the federal rules applying to discovery and deprived Defendant of representation. However, the judge denied the request for default judgement on the counterclaims noting that would be too severe given the facts.

This decision mirrors the apparent consensus on the state of inherent authority – that it is still available but limited. Judges are generally turning to inherent authority in a discretionary manner when the conduct is very egregious. While spying on a party to obtain information before discovery disclosure is a very severe action, other instances where judges have turned to their inherent powers include when a party withholds, loses, or destroys evidence.

Conclusion

The above represents a snapshot of two key discovery issues that persist before the courts. ESI protocols are increasingly pivotal in governing discovery disputes and judges are still turning to inherent authority to ensure all sanctionable discovery conduct is addressed. As remote work persists, technology usage evolves, and regulatory obligations tighten – there will be more cases in these areas and entirely new trends that unfold. Analyzing trends provides insight about investing in optimal technology and provider partnerships. Working with knowledgeable providers that have experience crafting ESI protocols, access to emerging technologies, and strategies to remain discovery compliant fosters successful streamlined litigation outcomes.

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.

California Cracks Down on Early Discovery Delays

Discovery abuse has always been a grievance for attorneys and judges. Delay tactics, overfull caseloads, inefficient time management, and even ill-intentions are reasons why the discovery process can drag on for much longer than it should. This wastes time, money, and other resources for everyone involved. It can even affect outcomes causing a party to settle or not be able to invest as much in a matter because too many resources were already spent on motions or other frivolous tasks.

There has been a growing trend of judges entering harsher sanctions to reach justice. Many are fed up with discovery abuses that not only prejudice the other party, but also impede the judge's ability to manage an overloaded docket. The state of California recently made legislative changes that feed into this trend and provide state courts with an opportunity to issue greater sanctions for certain discovery misconduct. California courts and litigators should become familiar with these changes before next year's effective date.

New California Law

On Sep. 30, the state of California passed a bill into law that increases sanctions for early discovery abuses and makes other significant changes. It amends the California Civil Discovery Act, which allows the court with party stipulation to order initial disclosures within 45 days. This includes but is not limited to contact information for anyone that is likely to have discoverable information with listed subject matter, relevant documents in the party's possession, and applicable insurance policies.

California courts now have the power to impose sanctions up to $1,000 when any of the following actions occur:

- Failure to respond in good faith to a request for the production of documents or to an inspection demand;
- Producing requested documents within seven days before the court was scheduled to hear a motion to compel that was filed due to failure to respond in good faith; or

- Failure to confer with the party or attorney that requested documents in an attempt to informally resolve any dispute concerning the request.

The prior limit for sanctions was $250, so this is a significant increase. Judges also have discretion to order sanctioned attorneys to notify the California State Bar within 30 days, as state law requires courts to report attorneys that receive sanctions of $1,000 or higher.

The new updates also add a section stating that each party must respond within 60 days after a party makes a demand for initial disclosures. The parties can stipulate to modify this arrangement and supplemental demands are allowed. This addition in itself is noteworthy as it highlights another key discovery trend – the desire for parties to be more collaborative early on in a matter without need for court intervention. This is added before the court order section, which sends a message that litigators should independently take advantage of early investigation to help streamline their cases. This could even provide information leading to early settlement, which saves party and judicial resources.

The amendments go into effect on Jan. 1, 2024. There is a sunset provision effective three years later that applies to all changes except those relating to increased sanctions.

Looking Ahead

The reason the California legislature made changes to the initial disclosure rules is to increase discovery efficiency, control costs, and attempt to put an end to unnecessary delays. Having some key information before getting to the actual discovery phase can allow claims with merits to get the attention they need, provide basis to perform early case analysis, and help judges maintain balance in their dockets.

California legislators have reported positive sentiments in hopes that these changes can combat some of the longstanding issues and provide benefits across the board. Adding caveats for supplemental requests and the sunset provision also offers room for everyone to learn during the process and make changes to the law if needed. It will be interesting to see whether more parties make demands earlier on and how judges enforce these provisions.

Other states with looser initial disclosure and sanction rules may also entertain similar bills, especially if the changes in California prove fruitful. Litigators should monitor this and be prepared to comply in the future. This is especially true since judges across the nation have been issuing harsher sanctions in recent years. Discovery cooperation has been an ongoing focus, but there could be more case law on the horizon about early intervention and disclosure mandates to achieve justice more expediently.

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.

AI and the Legal Profession: Hot Topics Before US Legal and Regulatory Bodies

The artificial intelligence (AI) wave continues to gain momentum as more organizations explore potential use cases. Generative AI specifically seems to be the topic of the year in the news, at work, and at home. Two common emotions seem to weave their way into every AI discussion – curiosity and fear. What business processes can these tools enhance? How can teams get buy in from their organization? There are questions posed by those eager to learn more and find beneficial ways to integrate AI tools.

Looking at the latter, there has also been skepticism about what generative AI can do and how risky it is to use this technology in business. Security, discriminatory outcomes, and privacy are all top concerns. What many are discovering that it is not the tool itself driving errors but instead the human behind the tech. Understanding how to deploy AI in a safe and responsible manner will breed success and highlight the importance of the human component.

Regulatory and legal bodies are recognizing that AI is here to stay. They are analyzing the benefits and risks from both human and technological standpoints. New legislation, regulatory rules, and court guidance can help organizations navigate AI and use these tools safely. Here are three hot topics in this area to monitor.

#1: State Legislation

It is unsurprising that that the states have started to consider and pass legislation on AI usage. This has materialized in several ways. One example is where states address AI via their broader state consumer privacy laws. Many enacted laws provide opt-out rights for using automated decision-making technology and profiling. Others require organizations to conduct risk assessments for certain processing activities where AI usage could fall into the proscribed categories.

Some states have additional laws on the books addressing narrow categories of AI usage. For example, in California the Bolstering Online Transparency Act requires organizations to disclose that communication is occurring via a bot when attempting to incentivize sale or influence election votes. There are also a few states that have laws placing restrictions on using AI for hiring purposes, including the Illinois AI

Video Interview Act. Also, the Maryland workplace AI law addresses the use of facial recognition technology during pre-employment interviews.

The above is only a snapshot and the beginning of what is to come. Since generative AI has taken center stage, more states have started to introduce AI bills. As of early September, there were 12 active proposed bills. Several others have been introduced over the past few years but have failed. The proposed legislation varies from focusing on generative AI to mitigating unlawful discrimination present in automated decision tools and much more.

Absent a federal law on AI regulation, the states will continue to attempt to pass their own laws. Some will be more tailored to specific topics or mentioned in broader laws. Other states may attempt to pass comprehensive legislation regulating AI. However, legislators and analysts are struggling with determining parameters that would embrace innovation without opening the risk floodgates. What may result is a patchwork approach to AI guidance that parallels consumer data privacy regulation.

A few predictions for 2024 are more focused AI bills, legislators and courts seeking education on use cases, risk assessment, and push for federal legislation. A few states have already created an unofficial group to collaborate on broad AI parameters. If this is productive, new bills will likely have some uniformity in terms of definitions and regulatory focus.

#2: SEC Conflict of Interest Rule

Regulatory bodies also recognize the importance of addressing AI and related technologies, with the Securities and Exchange Commission (SEC) recently voting to propose a new rule. If passed, the rule would regulate AI usage by broker-dealers and investment advisors. The SEC recognizes that firms have accelerated their use of new technologies. The SEC's fact sheet on this topic provides succinct reasoning for this proposal:

"When the use of these technologies is optimized for investor interests, it can bring benefits in market access, efficiency, and returns. To the extent that firms use these technologies to optimize in a manner that places their interests ahead of investor interests, investors can suffer harm. Due to the scalability of these technologies and the potential for firms to reach a broad audience at a rapid speed, any resulting conflicts of interest could cause harm to investors in a more pronounced fashion and on a broader scale than previously possible."

The proposal contains three main requirements. First, firms must neutralize conflicts of interest when using AI tools that advance their own interests over those of their investor clients. Second, to implement policies and procedures meant to prevent violations and comply with the rules. Third, to maintain clear recordkeeping when dealing with a conflict situation falling under the purview of these rules. According to the intended definition of covered technologies, the rules would apply to the major AI categories – reactive, limited-memory, and theory-of-mind.

The public comment period ends on October 10, so there may be some changes forthcoming. There has been some opposition that could influence the next steps. For example, opposers of the rule think this is a way to ban certain technologies. Also, that the rules could deprive investors of the benefits from AI when a firm opts out from using a tool to avoid costs associated with compliance. Interested parties should watch if the SEC formally adopts the rule over the coming months.

#3: Court Disclosure and Certification

Most have heard the story of the lawyer using ChatGPT to help draft a brief that ended up citing fake cases the tool created. This has caused several judges to implement standing orders requiring counsel to submit generative AI certifications.

Whether such disclosure is necessary is a prominent issue. This can promote the use of responsible AI by ensuring lawyers are reviewing the information that AI tools generate. This puts the court on notice, saves judicial resources, helps lawyers maintain reputation, and avoids delay.

However, many in the legal community have spoken out on the potential negatives of these orders. Some think they are duplicative. Another concern is that the lack of consistency may potentially cause mass confusion or make lawyers inclined not to use this technology in ways that it can be beneficial. The Judicature article "Is Disclosure and Certification of the Use of Generative AI Really Necessary" discussed potential alternatives. First, that it may be better suited for district courts to issue local rules on the use of Generative AI tools to promote uniformity and avoid adverse consequences. Second, that providing public notice may be a better route than creating new rules. This would include the already existing obligation to verify factual and legal representation when having assistance with drafting court filings, i.e., using generative AI tools.

While it will be interesting to see how the certification issue trends and evolves, the simple fact is that the responsibility to fact-check and provide quality control on technology output will always remain human responsibility. Lawyers must remain technologically competent and check their work or will otherwise face court sanctions, ethical violations, reputational harm, and lost business.

Conclusion

AI is going nowhere and will continue to be a hot topic for years to come. Staying apprised of issues before legislators, regulators, and the courts is not an option. It is imperative to be able to safely integrate emerging technologies into everyday business operations and maintain compliance across the board.

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.

Moving Information Governance to the Driver's Seat to Accelerate Cyber Breach Response

Information Governance often takes a back seat to other organizational initiatives. But why is this the case? The list of reasons is long and varied. Not knowing where to start or how to build strategic approaches to governing information are top contenders. It is important to understand how nuanced this concept truly is and how it is has shifted in recent years. Also consider what other initiatives may intertwine.

Harmonizing information governance and cybersecurity is a great place to start that will have an immensely positive downstream effect. This can minimize business disruption and regulatory risk while also improving ROI. Information governance is often viewed as discretionary spend, so combining with cyber efforts will increase ROI and outweigh any unplanned emergency costs resulting from a breach.

Modern Day Information Governance

Information governance encompasses the policies, processes, and controls that enable organizations to manage their information assets effectively. Many layers are involved as these initiatives need to address legal, regulatory, and compliance requirements while aligning information with business objectives. Take a look at the IGRM model that was revised last year to encompass all the components that feed into a robust and effective information governance program.

Information Governance Reference Model (IGRM)

This model illustrates modernized information governance. Priorities has shifted due to new tools for managing data, expanded use of AI for business processes, and ever-evolving legal and regulatory landscapes. Upon releasing this, the EDRM proclaimed: "Sound information governance is increasingly important in this information age, characterized by the proliferation of data, and the need for businesses to get the most value out of their data, while also complying with regulatory requirements, meeting litigation discovery demands, and protecting against security risks." It is no surprise that security was emphasized, as clear information governance is critically important to limit the consequences that could result from a substantial data breach.

Considering Cybersecurity

Cyber incidents happen daily. They threaten an organization's data management and retention capabilities, business operations, and client relationships. Significant liability can ensue after an attack, which has placed proactive breach planning as a top initiative for many. In IBM's 2023 Cost of a Data Breach report, 51 percent of organizations said they plan

to increase cybersecurity spending because of an internal breach. To bolster these efforts, information governance and cybersecurity need to intertwine.

Cloud-based information governance is trending in response to data privacy obligations, the need for tighter security, and ever-increasing amount of digital data. Being able to reduce breach risk by considering cybersecurity during cloud migration is an added benefit. Cyber insurance carriers are also imposing a higher level of scrutiny before writing a policy, so this is a way for organizations to illustrate strong security protocols.

As companies continue to move to the cloud and attempt to reduce spend on information technology, it is becoming more important to be creative in where investments are made across people, process and technology. Information governance is an area of opportunity to invest in to reduce the risk associated with cyber events.

Spend must also be thought of multidimensionally and holistically. Organizations must look beyond the cost to deploy and procure a solution. Increasing spend upfront in implementation and functionality can lead to reduced spend longer term by avoiding cyber events and minimizing the impact and cost of those that do occur. Think about costs associated with ransomware events, cyber counsel, business disruption to brand value, and the inability to do business for a period of time. The corollary of reducing spend also increases ROI, as tools bought for IT and privacy purposes may be applicable to security.

Exploring Solutions

An outside consultant can help mitigate the risk of cyber incidents by reducing the volume of data stored in a legally defensible manner. With stronger retention, organization, and encryption policies, there is less data available to intercept or access in the event of a breach. This greatly accelerates response efforts as there is less to sort through. This also offers deeper knowledge of where sensitive information resides and if it can actually be accessed by those outside of the organization.

Sometimes organizations already own technology that can help, but they are not taking advantage of the full potential. For example, in the Microsoft 365 environment there are several options available to better leverage an organization's investment in this technology.

Some areas to explore related to information governance include:

- Data Classification: Consider implementing sensitivity labels, sensitive information types, and trainable classifiers to foster cybersecurity readiness.
- Data Lifecycle Management: Leverage M365 retention policies and labels to place the organization in a better position to defensibly delete data and reduce risks associated with over retention.
- Records Management: There are file plan capabilities and label policies that allow organizations to build a comprehensive solution to manage business-critical data in compliance with regulations, laws, and unique records retention policies.
- Communication Compliance: Many organizations are faced with industry and government regulations requiring them to monitor and review a defined percentage of communications. This is to comply with industry regulations, reduce other areas of risk, and increase security. Leverage expertise in emerging technology such as Microsoft 365 to address these requirements and augment processes with staffing to manage overall workflow.
- Insider Risk Management: The single largest risk for data theft and leakage comes from internal staff, disgruntled workers, and employees looking to leverage corporate information at their next job. Most organizations are still taking a reactive and forensic approach to investigate insider risk. Predictive solutions become very cumbersome and expensive due to the volume of data that needs to be analyzed to identify risk. There are solutions that allow companies to identify triggers, trends, and events that often lead to data theft – or at the very least minimize or mitigate the loss when the theft occurs.
- Information Protection and Data Loss Prevention: Many organizations are faced with industry and government regulations requiring them to monitor and prevent dissemination of data outside of the organization. This includes HIPAA, Export Control, PCI, PII, and more. Managing and monitoring such data is of critical importance. Additionally, many organizations had to rush to cloud services during the onset of the pandemic to provide employees remote work access. Due to the expedited nature of migration, most concentrated

initial efforts on providing connectivity and securing authentication. Now these organizations are refocusing their efforts on protecting data. Microsoft and other tools offer solutions that allow organizations to identify sensitive data, monitor it, and apply protective controls.

All of this can feed into cyber initiatives by allowing organizations to leverage the value in their data while effectively managing security and compliance. Now is the time to move information governance out of the back seat and make it a key driver for cyber initiatives.

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 Future of Generative AI in the Legal Industry

Generative AI has taken the world by storm. A third of respondents in McKinsey's Global Survey "The state of AI in 2023: Generative AI's breakout year" reported regularly using generative AI for at least one business function. When looking at legal, business, and professional services 41 percent had tried generative AI at least once. Another 36 percent reported they regularly use it for work, personal use, or for both purposes.

These statistics are probably not shocking; what is surprising is how rapidly Generative AI is integrating into the business world – especially the legal industry that is historically slower to adopt new tools. Generative AI's transformation potential in legal is compelling. It is crucial to understand how legal is already using these tools, while also calling for transparency and to be conscious of ethical responsibilities.

The Current State of AI in Legal

The legal industry has embraced AI for years, as transformative tools and use cases continue to unfold and mature. AI tools are regularly used for document review, settlement evaluation, early case assessment, internal investigations, regulatory compliance, strategy decisions, and more. Seeing the benefits AI can offer has caused legal professionals to pivot and slowly turn an industry known for hesitation into one that embraces innovation. For example, AI tools have capabilities to detect and analyze data quicker and more efficiently. This has allowed lawyers to reallocate their workload, reach better outcomes, and tap into deeper business intelligence.

The rate at which organizations are already investing in generative AI is unprecedented, especially since this technology is still in the early stages and undoubtedly has more evolution in coming years. The ability to answer questions in a conversational manner and produce content based on prompts – in a matter of seconds – has caused mass intrigue. It will be interesting to see how this technology fits into already existing legal transformation initiatives and if the hype persists.

The New Frontier

Legal professionals should consider how generative AI can integrate into their workflows. The most significant short-term opportunities for both legal departments and law firms will likely be improving internal processes. Examples include generating reminders around security and compliance; information summarization across commercial contracts; incorporating generative AI into existing eDiscovery solutions; template creation; and brief drafting. Industry sentiment reflects this. In the 2023 Wolters Kluwer survey "Generative AI in the Law: Where Could This All Be Headed?" over 80 percent believe generative AI will create transformative efficiencies for research and routine tasks. Only 31 percent believe that AI will transform high-level legal work.

Imagine a lawyer preparing for a deposition. They're sifting through hundreds of emails, memos, and other documents to determine what can be disclosed and what must be kept confidential. Thanks to their organization's new AI assistant with advanced privilege detection capabilities, the lawyer receives a prioritized list of documents that are likely to be privileged. This allows them to quickly isolate sensitive materials and focus on preparing the deposition questions and strategy.

Today the AI assistant's capabilities extend beyond privilege detection. Amidst the pile of documents is a complex, 50-page contract that could be pivotal for the deposition. Instead of spending hours dissecting it, the lawyer uses the AI assistant's document summarization feature. Within minutes, the assistant generates a concise one-page summary, highlighting key terms and obligations. This enables the lawyer to grasp the essence of the contract quickly, integrating its crucial points into the deposition strategy.

The AI assistant can also flag any borderline cases for manual review, ensuring that the lawyer doesn't inadvertently waive privilege. This saves time and adds a layer of protection against potential legal pitfalls. By having a tool that can manage and execute routine tasks, the lawyer is left with more time to focus on value-driven work.

The above scenario reflects a day in the life of a legal professional that has successfully integrated generative AI tools into their regular course of business. It may be daunting when thinking where to start. To come up with the best plan, a good resource is talking to provider partners about how generative AI can solve current issues and close process gaps. They have the expertise to consult, implement, and monitor new technology investments.

Remaining Transparent and Ethical

While new AI technology holds great transformative potential, lawyers need to remain intentional when adopting new solutions. It is important to use these tools responsibly, being transparent with clients and upholding ethical duties. Risk analysis and policy creation are critical to fostering safe integration of new tools.

A recent Sedona Conference article by Hon. Xavier Rodriguez proclaimed that "AI is poised to re-shape the legal profession. But AI will require courts, rules committees, and ethics bodies to consider some of the unique challenges that AI presents. It will require attorneys to evaluate whether to use such products, and the risks associated with any use." In the McKinsey survey, only 21 percent said their organization has policies around using generative AI for work tasks. The top risk cited was inaccuracy, which only 32 percent of respondents said they were currently mitigating.

Consider the following ethical obligations:

- **Competence:** Lawyers must keep informed about innovative trending technologies and basic features even if not utilizing these tools, so monitoring generative AI updates is necessary.
- **Confidentiality:** Putting confidential client information into a generative AI tool can open the door to waive privilege and can violate the attorney-client relationship. Also consider the level of security and breach risk present before using a new tool.
- **Factual Discrepancies:** AI services may create untrue facts or leave out citations, but still appear convincing. This can result in violation of the ethical duty not to make false statements to the tribunal or third parties. Best practice dictates review of the facts to ensure they are accurate before filing with the court or transmitting to opposing counsel.

To remain transparent, notify clients of using generative AI on their cases and have policies in place to lower the risk of violating the above ethical rules. Also review public studies or testing data, talk to colleagues, consult with industry experts, or meet with counsel before making an investment to ensure that preferred AI systems promote transparency.

Regulation

To utilize these tools responsibly, having a framework for implementation is prudent. More U.S. lawmakers have been pushing for federal regulation to keep up with advancements that are changing the way people work, such as generative AI. While lawmaking can often be a slower process, the rapid adoption of these tools and push for regulation may expediate the process. The Biden Administration also issued an AI executive order on October 30 setting forth requirements for the government's use, evaluation, and procurement of this technology. It applies to over twenty federal agencies, but also provides requirements for certain private organizations. The order is comprehensive and includes directives on security, responsible innovation, competition, federal oversight, and much more. The President called out Congress to also act on regulating AI, which adds to the urgency.

Conclusion

It is becoming clear that generative AI is not just a tool but a partner in revolutionizing the legal industry. Legal professionals need to stay abreast of pertinent AI developments and consider how to thoughtfully integrate new solutions into their workflows. There will be a learning curve that will change over time as the tools advance, education ensues, and comfort level rises.

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 Evolution of Emojis in Litigation

Chances are most readers instantly associated meaning to each one of these symbols. Emojis are now a staple of modern communication. According to a recent article by USA Today, users share over 10 billion emojis daily across several platforms. Text messaging, emails, social media, documents, and work chat apps all have options to add emojis into communications. On July 17, many celebrated "World Emoji Day" for the tenth year. Each year more emojis introduced and are registered with Unicode, an entity attempting to standardize emojis.

All of this illustrates just how drastically communication has changed in a short period of time. Every year the use of emojis becomes more commonplace. This has presented litigation obstacles as the meaning of emojis is contextual and does not always mean the same thing. Take the first smiling emoji above. To some, this just conveys simple happiness or positive sentiments. However, other people attribute that particular smiley face to convey a passive aggressive or patronizing response. Also, emojis can look slightly different based on the device or operating system. See how it can get confusing when trying to decipher the context of a conversation during eDiscovery review?

There has also been a recent shift where courts are starting to give greater weight to emojis in their decisions. While this does not eliminate their subjective nature, it can cause disputes. Reviewing key case law and keeping apprised of best practices can help provide a roadmap for handling emojis during litigation. This will provide insight into how courts may handle key issues, while also offering guidance on how to practically approach emoji review.

Compelling Case Law

Recent decisions in the U.S. and abroad highlight the prevalence of emojis in modern communications. Judges have accepted that these symbols carry meaning and in some situations are finding them legally binding or otherwise significant.

Here are three examples of this sentiment in practice:

1. In the case of *In re Bed Bath & Beyond Corp. Securities Litigation*, 2023 U.S. Dist. LEXIS 129613 (D.D.C. July 27, 2023) the court denied a motion to dismiss in a securities fraud case. Bed Bath and Beyond investors brought a class action against Ryan Cohen for securities law violations. He made $68 million in profit after talking up the stock and then liquidating. He tweeted a message with the full moon face emoji, which plaintiffs interpreted as a sign to hold or buy the stock because it would go "to the moon," thus driving up the price of the stock quickly. Cohen maintained that this was ambiguous, but the judge pointed out how important context is in this situation. Also, how language in itself can be ambiguous and contextual depending on tone, sarcasm, and the overall situation in which relaying a message.

2. In Canada, the judge in *South West Terminal Ltd. v Achter Land*, 2023 SKKB 116 (CanLII) ruled that the "thumbs-up" emoji was sufficient to demonstrate contract acceptance. The court granted summary judgement placing $82,000 liability on a farmer that breached a contract by failing to deliver goods to a buyer. The buyer texted a photo of their contract and said, "Please confirm flax contract." The farmer responded with the thumbs up emoji, arguing that this was meant to convey receipt of the text but not a digital signature. The court did not find the intent relevant

and found that although untraditional, the circumstances warranted interpretation that this was a valid signature.

3. In *Rossbach v. Montefiore Medical Center,* No. 19-cv-5758 (DLC), 2021 WL 3421569 (S.D.N.Y. Aug. 5, 2021), the judge issued an instructive opinion on emoji review. The plaintiff filed a wrongful termination suit where she claimed sexual harassment. In discovery, she produced text messages from a former co-worker going to the core of her claim. Defendants reviewed the produced text messages and raised several issues with their credibility, one being the characteristics of the heart eyes emoji image. The judge found that plaintiff fabricated this evidence and ordered dismissal and monetary sanctions. Analysis of the emoji was pivotal to this decision, as the characteristics were inconsistent with what it should look like on the phone's operating system.

   In August 2023, the Second Circuit upheld the case termination and monetary sanction against plaintiff but vacated the sanction ordered against her attorneys. It noted that the lower court incorrectly applied the wrong standard, which should have been explicit bad faith.

Tips for Success

Emojis will only continue to integrate into modern communications. This means that they will keep coming up in litigation over text messages, emails, work chat apps, social media messages, and more.

To ensure proper handling of emojis during litigation, take inspiration from the case law above and consider these suggestions:

1. Understand that emojis will always be contextual. While some have a more universal meaning, others are subject to the user's interpretation. This will warrant manual review to some degree, so make sure to include that in eDiscovery workflows. This also may require a specific line of questioning during depositions or trial to garner the correct context.
2. Consider the different characteristics emojis may have over different versions of an operating system or devices. As Rossbach illustrated, emojis can be a pivotal source of evidence and having the right review skills is crucial.
3. Litigators should take reasonable steps to affirm authenticity of the evidence their client provides. Although sanctions were overturned in the Rossbach case, another judge could rule differently. Even if a court requires demonstrative evidence that an attorney acted egregiously in order to issue monetary sanctions, negligent or reckless representation can still result in discipline before the state bar for ethical violations.
4. Looking through a wider lens than discovery, the other cases discussed above illustrate how emojis can come into play dispositively. It could support or defend against certain motions, which means that an earlier understanding of key communications may be necessary.
5. Look for a provider that offers an end-to-end chat data eDiscovery solution' that can help with production, assist with contextual review, and consult on litigation trends. For example, using tools that have capabilities to render emojis inline can be very helpful in deciphering context. This will allow reviewers to view collaborative chat conversations and instant messages as if using the custodians' native chat applications with all the nuance and interaction needed to make sense of modern messaging.

Incorporating these tips into practice can improve approaches to eDiscovery and litigation as a whole. The case law on emojis will also keep surfacing, so make sure to read them to remain informed on new guidance in this area.

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.

Blockchain Considerations for Litigation and Investigations

More organizations continue to adopt blockchain technologies. According to Grand View Research, the global blockchain technology market value was estimated at 10.02 billion in 2022. Analysts forecast a compound annual growth rate of 87.7 percent between 2023 and 2030. Cryptocurrency holds the top spot for blockchain in business, but other use cases are growing in popularity. Sectors embracing these technologies more frequently include financial services, government, and healthcare. The market opportunities will only continue to expand as interest and knowledge persists.

So, what is so appealing about blockchain? Looking at the inherent operational features will answer this question. It allows users to record transactions securely and permanently over a distributed network of computers. There is no need for a third-party facilitator and the transaction history is immutable. Think of a financial institution adopting a blockchain payment system to facilitate global transactions. This can enable cross-border transactions with ease. Other trending use cases include smart contracts, cryptocurrency payment for services, cryptocurrency-backed financing, and security enhancement.

As with all emerging technologies, there are special considerations when dealing with litigation or regulatory investigations. Blockchain has come up more frequently as discoverable ESI alongside increased adoption. Agencies like the SEC and CFTC are opening investigations more often to ensure crypto exchanges and organizations utilizing blockchain technology are acting appropriately. One example is an investigation into an organization's initial coin offering.

Anticipating Challenges

All new data sources today pose some level of collection and review challenges. Blockchain is no exception, especially since the technology behind it is unique and complex. It is crucial for an organization's legal department to remain informed and work with their entire enterprise to develop blockchain-specific policies. There are implications for forensics, information governance, eDiscovery, privacy, and compliance. This can be a lot to juggle, especially when the department lacks deep expertise of unique issues that touch these areas.

Finding the right partnership can make a world's difference. Here's why.

A provider with blockchain experts can advise on litigation and investigation implications, allowing the organization to gain a strategic advantage and be armed with key insights. For example, getting advice on what to be mindful of when deploying or encountering blockchain technology and proactively accounting for this in information governance plans can be a game changer. This approach will help limit future eDiscovery issues by knowing where data is located and having policies around storing sensitive data types in this technology. Generally, with encryption blockchain is deemed usable for storing sensitive data. However, organizations should think through this carefully. There is ongoing discussion about whether it is appropriate to keep certain data, such as medical information, on public blockchain.

Forensic capabilities are crucial for eDiscovery as tracing transactions within a blockchain can be challenging. Depending on the organization's level of blockchain involvement, a managed services offering may prove ideal. Make sure to ask potential provider partners not only about forensic collection and analysis skills, but also about approaches to transaction lifecycle tracing and data preservation. All of this will contribute to a strong strategy for blockchain-related litigation and investigations.

Lastly, legal departments need to remember that they may encounter blockchain as an ESI source even if their organization does not utilize this technology. The opposing party – or even an uninvolved entity – may have relevant information located on a blockchain network. For example, last year in the fraud case Jacobo v. Doe a judge allowed a party to serve discovery requests to cryptocurrency exchanges to help identify an unknown defendant. This is also instructive as it provides litigators with new avenues to explore when identification issues arise, as cryptocurrency transactions are permanent and unable to be altered.

Final Thoughts

In sum, when new technology is adopted, the legal implications should always be addressed proactively. Failure to do so can have negative consequences that would otherwise be avoided with the right resources in place.

With the fall of the FTX and other crypto exchanges, there will be more regulatory scrutiny around digital currencies and blockchain. Therefore, informed usage of this technology is an absolute must. Organizations and their legal departments need to become well-situated to embrace these technologies where appropriate and have partnerships in place to overcome the hurdles.

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.

Forging a Path Forward When Legal Tech Fumbles

The use of legal technology is up 53 percent as more legal departments are searching for new ways to use these tools to manage their workflows, according to the Thomson Reuters 2023 Legal Department Operations Index. This is not surprising as innovative tools continue to enter the market and there is more eagerness across the board to derive the benefits. Smaller and medium sized organizations are joining larger organizations in the building of their legal operations teams and tech stacks to enhance their environments with foundational tools such as contract management and matter spend management.

But what happens when a technology initiative does not live up to the expectations? This a common refrain amongst many corporate legal leaders. A lot of time and resources are spent on tech investments, so underperformance can be disheartening. It can be difficult to determine the underlying reason for the investment going off course.

It often is also tricky to determine the best path forward. Is it time to scale down the tech the department already has in-house? Would revamping current usage with new processes and efficiencies be a better option? Is it time to throw in the towel and start over with a new tool?

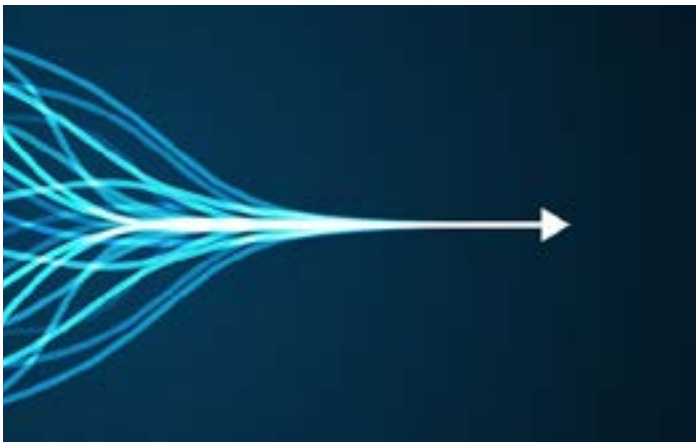
To answer these questions, it is first crucial to pinpoint why a tool is underperforming. Then, how to determine whether to optimize existing technology or start over with a new solution.

Common Obstacles

When diving deeper into why a tool is not living up to expectations, it frequently becomes clear that the technology itself is not the issue.

Here are three alternate reasons to consider when researching the root cause of a seemingly failed legal tech investment.

- The business case projections may have been too ambitious. A reassessment may show that an extended timeline or refocused use cases would lead to better results.
- The manner in which the vendor implemented the tool was not up to par with what the organization needed for it to thrive. It is important to thoroughly vet partnerships and have discussions around implementation beforehand in order to appropriately align expectations.
- The internal processes around using the new tool were weak or unclear. Change management can be hard. Even the best tools in the market can underperform without proper usage, training, and stakeholder involvement. This leads to people giving up and sticking with the old ways of completing tasks.



Considering the above will often show that the technology was not a failure at all. Instead, it is time to evaluate tech performance through a different lens to pinpoint valid feedback and determine where implementation or utilization fell short.

Cultivating Successful Outcomes

There is one questions that ensues: is it time to turn back or push forward? At this point, it should be clearer how the organization is actually using current technology and it is time to set some goals for the future. Whether to optimize current tools, drop them, or invest in new tech will be the focus. Best practice is to optimize what the department already has, then look to new solutions if necessary. Optimization versus new investment costs, need for data migration, internal compliance, and change management sentiment will all feed into this assessment.

Three factors will guide this decision: technology roadmaps, process mapping, and stakeholder engagement.

Technology Roadmaps

Having a functional detailed plan is crucial. Building a legal technology roadmap with clear goals in mind leads to improved operational performance management. When a tool underperforms, it is time to dive deeper. It may become clear that it is time to redefine the roadmap in order to determine the best path forward. While all roadmaps are unique and require room for change, consider including the following characteristics:

- Define a phased timeline that supports iterative development and leaves room for evolution. A major roadblock to successful implementation is attempting to accomplish too much too quickly.
- Focus on the tool's enhancement capabilities instead of strictly looking at the functionalities.
- Consider the broader technology stack and architecture for both the legal department and entire enterprise. This will help avoid siloed operations and disjointed technology integration, while also shining light on other potential opportunities.

If these things were not done at the outset, it may be why the technology did not live up to the set expectations. Redefining the roadmap to incorporate these factors may provide an opportunity to push forward with the investment and avoid the need to be reactionary when something goes off track. Always include room to reprioritize.

Process Mapping

Teams may avoid mapping out processes before integrating new technology because it can be time-consuming. However, failing to do so can lead to confusion over how to effectuate meaningful change and achieve uniform adoption. Process mapping will show how the department operated before the new tool came aboard and throughout the integration process. This can inform decisions about how teams can do things differently using the current technology investment, where gaps exist, and whether it is time to take a new path.

Stakeholder Engagement

Take a look at the level of stakeholder engagement during the tech planning, implementation, and follow-up phases. These individuals need ownership and say for a tool to thrive. When key stakeholders are involved, it is easier to get the resources and training necessary for teams to effectively integrate new solutions into their workflows. A huge roadblock to effective change management is when there is lack of stakeholder involvement and commitment to helping carry out the change.

Stakeholders should be ready, willing, and able from day one to embrace everything that goes into adopting and successfully integrating new technologies. To attain this, consider these best practices:

- Identify stakeholders and determine how much support and influence they can offer for the project. Build an initial strategy around getting the right stakeholders on board and well-positioned to effectuate meaningful change.
- Perform change impact and change fatigue assessments. These bring to light how many different areas across the enterprise that changes to technology and process will touch, how significant the impact will be, and where to proactively create mitigation strategies.
- Create a clear vision so there is a collective understanding of how to achieve success. Hallmarks of a successful plan include specific and actionable goals, considering the entire organizational architecture, and engaging pertinent stakeholders optimally at each stage of the process.
- Thoroughly communicate what each business unit needs to do before a new tool launches and schedule trainings.
- Create a continuous operational improvement plan to keep on track, measure success, receive feedback, and make revisions based on user input.

All of these steps will be more impactful with informed and engaged stakeholders taking purposeful actions to ensure a new tool thrives.

Conclusion

Following the steps above will help legal departments better evaluate their legal tech stack and make more strategic decisions in the future. In many cases, they will likely find room to optimize – at least to some degree. There are also external legal business advisory resources that can help navigate tech initiatives and redefine strategies with ease. All of this will make everyone happier and create an internal culture of more informed and tech-savvy individuals.

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.

Looking at Data Breach and Class Action Exposure Through a Single Lens

There has been a spike in data breach class actions this year. According to a study by Law.com Radar, the monthly average of data breach class actions was 44.5 from January through August. This figure is more than double of last year's 20.6 monthly average. Data breaches have also been on an uptick. According to the Identity Theft Resource Center, there was an increase of 114 percent in reported data compromises from 2023 Q1 to Q2 reflecting the highest number of breaches ever during a quarter. These incidents are getting more costly each year. IBM reported in the 2023 Cost of a Data Breach report that the global average breach cost was $4.45 million, representing a 15 percent increase over three years.

But what do all these statistics mean and how should business leaders react? First, it is time to come to terms with the reality that any organization is fair game for an attack. They must pay attention to the data breach class action landscape. Next, instead of viewing these trends in isolation, it is time to unite them and look at the whole picture. Where significant data breaches occur, class action exposure increases exponentially. Lastly, organizations need to formulate a breach response plan that is proactive, accounts for risk mitigation, and factors in potential class action liability.

Current Conditions

There are several factors contributing to the rise in data breaches. The obvious reason is that as the world continues to digitize more, there is more information out there to access. Bad actors are developing more sophisticated and strategic ways to target sensitive information, while organizations are simultaneously producing and storing a record amount of data. They are also figuring out how to use advanced technologies as a tool to intercept information.

For example, ransomware attacks have been trending in recent years with demands previously in the thousands now in the millions. Even if an organization saves money by paying the ransom, this is contributing to the bigger problem. Bad actors will keep perpetuating these attacks because they have gotten away with it in the past, while continuing to sophisticate their efforts. Other trending attack methods include phishing, multifactor authentication breaches, and malware.

Large-scale hacks have also contributed to the drastic uptick in breaches. The MOVEit hack resulting from a software vulnerability that began in May 2023 (and is still ongoing) is one of several recent events illustrating how widespread attacks can quickly place a large number of organizations at risk. Many MOVEit incidents involve over one million impacted contacts and the types of data impacted tend to be rich files with complete contact data, such as complete client or employee lists containing full PII sets. Events like this have the potential to create large class action lawsuits against the software creator and its customers. Affected individuals have already started filing lawsuits against organizations using MOVEit, thus highlighting the importance of not only having sound internal practices but also keeping apprised of third-party systems storing any business data.

The above coupled with more court education, regulatory rules, cyber insurance mandates, and media reporting on data breaches highlights how front and center this topic is currently. This has directly caused more class action activity that is costlier. Settlements are higher due to the number of affected consumers and public attention on breaches of all sizes. More class actions are being filed and courts are allowing certification. The Law.com Radar study found that from this January through June there were 246 data breach class actions, which is close to 2022's grand total. Courts are even requiring defendants to turn over privileged investigative breach reports.

These circumstances place urgency on breached organizations to mitigate quickly and explain security gaps to save their reputation. To lessen risk, it is crucial to not only anticipate data breaches – but also the class actions that can follow.

Adapting and Acting

It is time to act. Having controls in place to mitigate breach risk is no longer an option. Organizations must review their security gaps regularly and make this an ongoing top initiative. Not putting enough prevention in place to avoid a breach or failing to quickly determine a breach cause and remediate it effectively are both contributing factors to the uptick in class actions. However, more are looking to invest in cyber preparedness as demonstrated in the IBM report where 51 percent of organizations said they plan to increase cybersecurity spending because of an internal breach.

But where to start? Keeping on top of the changing landscape will help improve policies and procedures related to managing threats and risks, but this is only the beginning of what needs to be done to have a robust and effective cyber readiness plan that also anticipates class action activity. What needs to be done will be unique to every organization. The goal should be to determine the best combination of security controls that fall within an organization's risk tolerance. From training to threat detection software, mock breach exercises, and beyond – the possibilities are plentiful and flexible.

This is not a feat to tackle alone, so fear not. An outside consultant with not only cybersecurity capabilities, but also class action, is ideal. Look for an expert partner that can pinpoint cyber gaps and fix them by integrating new tools or information governance approaches; advise on what to include in an organization's incident prevention and response programs; keep apprised on breach and class action trends; provide breach response services; and have staff available to handle class action administration in the event that one materializes after a breach.

By tapping into outside resources in addition to internal efforts, an organization will be in the best position to tackle data breaches that come their way – and any class actions that may follow. This will also reduce breach and class action risk in the first place, providing peace of mind and allowing organizations to maintain good cyber hygiene.

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.

Minutes Matter in Modern Legal Practice

In litigation and investigations, every minute matters. Having access to information at a moment's notice can be critical. Imagine, a settlement agreement comes in after hours and the partner on the case needs to know the amount spent to date on the discovery component of the case right away. Let's say you are in-house counsel overseeing a massive investigation and need to report to the business side in a matter of minutes the status budget of the case. What do all of these situations have in common? Each person needs immediate access to their data.

In today's legal climate, easy access to metrics matters. There are so many potential instances where having data at your fingertips can help quickly guide strategy and make informed decisions.

Transformative Opportunities

Seeking out innovation is crucial to thrive in the era of modern law. Litigation and investigations are picking up speed and there are more case demands. Many law firms have gone global. Remaining informed, having access, and being cost-conscious are important. These are key drivers in the practice of law today, which now encompasses the need to innovate and view matters through a strategic business lens.

Lawyers want and need readily accessible data to make key decisions about their cases and facilitate new ways of working. In a dynamic and collaborative workspace, it is crucial to have access to all data versus merely relying on what a particular team member has saved on their desktop. One way to increase efficiencies is through technology and partnerships. This can help fill process gaps, eliminate challenges associated with time zones, and overcome roadblocks to information access.

Choosing the Right Solution

Having confidence and visibility into the backend infrastructure that any business partner deploys is a necessity. Law firms and corporate counsel must keep this in mind when choosing an alternative legal service provider (ALSP) for litigation and business needs. Look for a strategic partner that

offers a dependable, modern global infrastructure. But what does this look like? Here are some features that fit the bill.

- The capability to seamlessly integrate services and technology into an organization's internal infrastructure and security controls.
- A modern cloud platform that provides ease of use and access to all information that the ALSP manages for the organization. Some key components to look for are single sign on, user support, client visibility, application access to view all case data, on-demand reporting, and mechanisms to submit requests.
- Solid security controls that provide peace of mind that client and other sensitive data is safe. With hackers looking for any way to get personal information and regulators cracking down on data privacy, this should always be a top priority.
- The use of best-in-breed technology to create interactive business intelligence reports. The ability to access analytical reporting empowers organizations to make better business decisions.
- Customization options so organizations can mix and match services with ease. Every case is different and organizations have varying approaches on how to handle matters.

Having a strong cloud-based data management platform providing instant access to data enables corporate legal departments and law firms to meet deadlines, capture institutional knowledge, and derive actionable insights from comprehensive data analytics. In a legal climate where minutes matter, this is an invaluable tool that not only will redefine the ALSP relationship but also foster 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.

Ready For Some More Holiday Cheer? Check Out Epiq Angle's Top Blogs From This Year!

The end of the year always brings opportunity to reflect. Keeping with tradition, we analyzed the traffic to our 2023 blog posts to see what piqued our readers interest the most. What we found was a focus on innovation for legal and business processes. With transformative technologies like generative AI trending, risk and benefit analysis are crucial. Factoring in cybersecurity, information governance, economic conditions, and the value of actionable business intelligence is key. This helps organizations develop better strategies around embracing innovative technologies, remain compliant, control costs, and safeguard data.

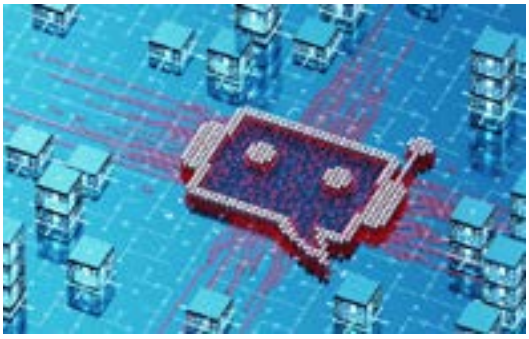
We hope our readers have enjoyed the array of topics in our blog this year and are excited for what 2024 will bring. To all of you checking out the Epiq Angle, we hope your holiday season and new year is filled with joy. We appreciate your continued support!

Take a Look at This Year's Trending Topics

The most popular topics from this year included generative AI, cyber attack methods such as deepfakes, the intersection of information governance and data security, the role of ALSPs in today's legal climate, and current bankruptcy trends.

Here are links to five of our top blogs from this year covering these topics:

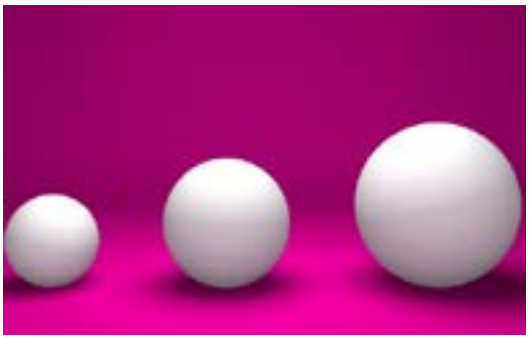
Generative AI and Business: The Basics and Benefits – Part 1



Deepfakes Bring Deep Risks

Minimizing Data to Minimize Exposure: Information Governance and Data Security Overlap

Welcome to the Third Generation of ALSPs: The Future of Legal Service Delivery



Correlating Commercial Real Estate and Bankruptcy Trends

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.