Inside 1Q2019

ACC Association of Corporate Counsel
ARIZONA

FOCUS

President's Message

Mark Rogers

Many thanks to Casepoint, Ogletree Deakins, Ryley Carlock & Applewhite and Snell & Wilmer, for the articles in this newsletter! We also want to thank them for presenting excellent CLE Programs for our Chapter! We hope you will find their articles a useful resource.

We are halfway through our 2018 – 2019 year and are in the thick of our Ethics CLE offerings. We expanded the number of ethics hours available this spring to help meet the increasing demand for Ethics credit as well as to provide more scheduling flexibility for you.

We are continuing our member attendance incentives with door prizes at each meeting. We have some great prizes queued up for the next quarter! Watch the weekly emails for details. Registration for meetings opens four weeks before the meeting date. We have included the CLE schedule for next quarter in this newsletter. Please plan to join us.

The 2019 Arizona Corporate Counsel Awards were held on January 17. Our gratitude to ACC AZ Chapter Board member, Sasha Glassman, for once again working for several months to make this event a great success!

Congratulations to all of the 2019 Award winners:

Public Company: **Sonny Cave**, ON Semiconductor

Up-and-Comers: **Ijana Harris**, Maricopa Integrated Health System and **Matthew Meaker**, Sundt Construction

Pro-Bono Award: **APS/Pinnacle West Capital Corporation Legal Department**

Government, Municipal or Public Sector: **Michael Minnaugh**, Valley Metro

Nonprofit Sector: **David Mulvihill**, Make-A-Wish Foundation of America

Private Company: **William Sawkiw**, Bar S Foods

Medium Private Company: **William Black**, MD Helicopters

Large Private Company: **Jeff Hansen**, Troon

Legal Department of the Year: **Microchip Technology**

As we mentioned in the last newsletter, this year the ACC Annual Meeting will be held in Phoenix during the last week of October 2019. We are busy planning a special event with our sponsors that will Celebrate State 48! Watch for more information as we finalize our plans. The early bird discount registration for the Annual Meeting ends this month! If you have not yet registered, please take advantage of this discount before the end of March.

As always, thank you for your loyal support of the Chapter.

See you at a Chapter event soon!

Please plan to join us for our upcoming meetings:

April 4, 2019 at The Capital Grille
MEMBERS ONLY CLE: Brand Protection Strategies OR Protecting Your Employees & Company from Workplace Violence

April 11, 2019 at The Capital Grille
MEMBERS ONLY CLE: Issues and Pitfalls to Avoid when Drafting and Litigating Indemnity Clauses

April 16, 2019 at Blanco Biltmore
ETHICS: Crisis & Investigation Management in the Era of 24/7 News Cycles

April 23, 2019 at The Capital Grille
MEMBERS ONLY CLE: How to Limit Liability & Risk in Your Foreign Operations

May 2, 2019 at The Capital Grille
MEMBERS ONLY CLE: Protecting Employer IP, Reputation, & Office Culture without Violating Employee Speech Rights OR TBA

May 9, 2019 at The Capital Grille
MEMBERS ONLY CLE: Advantages & Disadvantages of Involuntary Bankruptcy Filings as Debt Collection Strategy

May 14, 2019 at Blanco Biltmore
Managing the Unmanageable: Difficult, Toxic & Gotta Go Employees

May 21, 2019 at Blanco Biltmore
ETHICS: Internal Investigations & the Attorney-Client Privilege - I'm Covered, Right?

June 6, 2019 at The Capital Grille
MEMBERS ONLY CLE: Trans 101 for Employers OR Best Practices for Corporate Political Involvement

June 18, 2019 at Blanco Biltmore
ETHICS: Ethical Issues - Can They Really Do That? Ethical Minefields & How to Dodge Them

Top 5 Legal Tech Trends to Watch in 2019

By K Royal, TrustArc.

Technology rules the world, and the legal world is no exception — from commodified personal data to artificial intelligence (AI) to security. So, what are the hottest legal tech trends we will see in 2019? To answer this question, we must review the growth of technology over the past few years.

I searched for an article written within the past 10 years, and found a 2011 piece from the American Bar Association entitled, "What's Hot and What's Not in the Legal Profession." Privacy was not listed, much less cybersecurity. Yet, these have been driving forces in technology, particularly legal technology, for years now.

As technology has advanced, privacy and related fields (e.g., security, data protection, cybersecurity) have become the fastest growing areas of law. Here's how they have evolved and what we might expect in 2019.

1. Security and fraud prevention

Protecting data, in any form, requires security measures. Additionally, there is an increased focus on cybersecurity. The number of breaches has been steadily increasing, including ransomware, malware, and corporate espionage.

Among the largest security risks in recent years was the alleged infiltration of US companies by Chinese hackers who installed microchips to server motherboards sold to many US companies. Whether the microchips actually did exist or not is not the main point; the crux was how the potentially impacted companies and the various government agencies responded. This incident also highlighted the heavy reliance US technological supply chains have on products from a handful of countries, including China.

With the Internet of Things (IoT) so prevalent, the supply-chain concern may have a huge impact on the security of devices, including infected personal devices connecting to work environments. This is aside from employees stealing data, such as the 50 terabytes found in the home of former US National Security Agency employee, Harold Martin.

This level of technological manipulation has made fraud easier to commit. Companies are taking steps to prevent and identify fraud, especially with artificial intelligence (AI) capabilities, yet fraud will continue to grow.

Many companies worry that the General Data Protection Regulation (GDPR) will impact their fraud prevention efforts due to its granting the individuals' control over their personal data, such as access, rectification, and erasure. Preventing fraud is likely a valid reason to deny such rights, but companies must consider its programs, the information obtained and retained, and prepare defenses for its activities.

Many regulations now require protection for personal data, but often do not specify the security controls. The ones that do, such as the US Health Insurance Portability and Accountability Act of 1996 (along with its subsequent amendments, HIPAA), may be outdated (but there is a current Request for Information issued by the US Department of Health and Human Services addressing areas for HIPAA to be updated).

Instead, the standard generally requires reasonable security relative to the size of the company, its resources, the level and amount of sensitivity of the personal data, and the industry norms. This is a target in motion that will ebb and flow with the issuance of regulatory guidance, court decisions, publicized breaches, and technology growth.

Technological advances breed opportunities, for both good and bad actors.

2. Data governance

Often, people confuse data governance with data protection. Data governance is a much larger field, although a good data protection program includes good data governance and vice versa. Data governance is a programmatic concept that focuses on personal data from its inception to destruction — cradle to grave. Therefore, it comprises availability, usability, integrity, consistency, accountability (auditability), and security.

In many cases, companies developed data governance programs in specific data environments or for specific regulations, such as HIPAA, the US Sarbanes-Oxley Act, or various physician payment reporting requirements. Data governance is particularly challenging in an environment that has historically relied on paper documents, but a solid data governance program will help reduce document proliferation, both physically and electronically.

However, given the importance and vulnerability of corporate confidential data (the "crown jewels") along with far-reaching personal data laws, like the GDPR and the California Consumer Privacy Act, companies should adopt a full-scale data governance program. We are seeing this happen specifically with the GDPR, where companies are creating data inventories and records of data processing activity.

continued on page 3

continued from page 2

Data inventory, though tedious, is a fundamental element of data governance. How can companies protect what they don't know they have? Once there is a data inventory, companies should launch programs, such as data protection impact assessments, privacy impact assessments, vendor classifications and oversight, and retention and destruction policies and schedules.

Companies should invest in technology for these purposes, such as dynamic, user-friendly data inventory systems like the TrustArc Data Flow Manager, which links to DPIAs and vendor assessment tools. Other technology options include Truyo, which offers robust solutions for automating data subject access requests and Exego, which provides intelligent, automated analysis of unstructured data. A manual program in spreadsheets and paper only works for small companies with minimal data and vendors.

Certainly, a data governance program should come with someone to lead it. Whether the company needs a privacy officer, security officer, data governance officer, or information security officer, a data protection officer (DPO) is a determination the company needs to make.

Likely, it is a combination of roles that is required. The individuals chosen as DPOs must keep both privacy and security in mind. Multiple individuals may have the expertise, in whole or in part, to become or to assist the DPOs. Remember that the DPO is a role required under GDPR if a company meets certain thresholds.

If a company appoints a DPO voluntarily, even without meeting the thresholds, then the DPO and the company are held to the same standards as if a DPO were required. So be careful what title is used. But more importantly, be clear on the scope and responsibilities of the position.

Regardless of the role, the position must carry both authority and accountability within the data governance program. Accountability without authority to make decisions, maintain a budget, and execute the duties of the position makes it a position in name only — an empty suit — and is useless in building an effective data governance program.

3. Automation

Technology is both the goal and the tool to achieve it. Automation currently plays a key role in machine learning (or AI), marketing statistics, fraud detection and prevention, targeted behavioral ads, and much more. We will see this trend continue to grow.

We have seen automation in place to handle risk assessments for personal data, risk-based business acceptance, consumer and client self-service portals, contract lifecycles, and work process templates. By using automation, companies can easily scale up their efficiencies, serve more clients (internally and externally), and create outputs and metrics to determine the best use of resources.

AI can help manage large volumes of information quickly and be programmed to deliver necessary information, such as contracts. For example, with some software, such as the Exego platform mentioned above, you can check breach notification timeframes or limitations of liability clauses across 3,000 contracts within seconds.

Templates are one of the easiest ways to enter the automation workstream for in-house counsel. Most of us have standard agreements already, but what about automating flexible agreements that can easily suggest or adjust approved clauses, complete terminology changes, and attach the right geographical or product requirements to all necessary documents?

The software would also help the legal team to identify what clauses are consistently problematic across the client base. Once in place, those pesky conditional requirements could be automatically triggered to ensure vendor A got its audit report submitted or vendor B moved to a lower cost for a higher-quantity purchase.

Another area for automation focuses on individual rights to data. Automation can be used to handle intake requests, show the requestor what is available, and process requests according to a set of parameters. One could carry this further and have product teams input certain information, such as personal data elements (e.g., name, location, tax identification numbers) and geographies, and then generate a privacy notice.

An interesting aspect of automation is legal project management. This software is starting to be used more commonly in law firms, but there is no reason that it would not also help streamline the workday of in-house counsel. This particularly helps if counsel have project-type work with multiple actions by counsel to complete, such as implementing policies across multiple jurisdictions, mergers and acquisitions, and product development lifecycles. Given the increasing amount of work we are seeing in-house, tools to assist in organizing our workstreams could be useful.

The last example in this segment is online or phone helper bots. Your company may consider using these tools, and in-house counsel need to understand the technology (see the "Tech and data fluency" section below) for the benefit of the external clients, to prepare notices, and to comprehend any potential liability. But perhaps these technologies could also benefit in-house counsel in their duties.

4. Mobility

Mobile workforces and devices are certainly not new, but we are seeing the concept of mobility increase and impact even more areas of our professional and personal lives. Cloud services are ubiquitous, and the growing expectation is that one truly can work anywhere at any time with access to shared drives and real-time collaboration online available on any computing device.

Phones can now store up to a terabyte of data. In context, a terabyte is roughly the equivalent to 40 Blu-ray movies. This poses an increased security risk that in-house counsel can't ignore.

We see the complexity of the risk encompassing a company's mobile device management, data loss prevention, remote access, outsourced cloud services, audit trails, disaster recovery, back-up, data retention, and data and device destruction.

But let's take the hypothetical further by adding driverless cars, smart homes, and trackers (like mobile employee badges for easy access to satellite offices, hotel entry keys, and keyless cars). Will mobile devices

continued on page 4

continued from page 3

sync with one's environment to facilitate a merger of work and life? Imagine leaving work with some tasks to do, perhaps a contract negotiation.

Enter your driverless car, where you take a call and the contract displays on an inside wall, muting traffic noises, and reflecting changes captured orally, noting who suggested what and who agreed. Dinner choices pop up on a side screen, so you can choose your meal to be delivered 30 minutes after arriving home, given current traffic conditions.

Once home, the dog's kennel unlocks, your call switches to the house phone, automatically muting on your side to give you time to get settled. The contract shifts to the screen of each room you walk into for seamless viewing. Your evening beverage dispenses, while the home temperature changes to "at home" settings. Meanwhile, your significant other is alerted that you have arrived home, dinner has been ordered, and you are scheduled to be on a call for another 20 minutes.

We enter a mobility ecosystem with a new infrastructure, perhaps built on existing technology and incrementally moving us from one state to another. Alternatively, the new infrastructure may change drastically, thanks to technologies that disrupt our industries, as the mobile phone has done. We may not see the full-scale mobile ecosystem arrive in 2019, but the scenario above is imagined with, and based on, current, known technology.

5. Tech and data fluency

It's imperative to be fluent with technology and data and our devices must be fluent with each other — except where it should be prohibited. Common prohibitions would be set by the corporate data classification, where the most sensitive data— draft product development, strategic plans, and sensitive personal data — would be restricted to identified devices and not shared. Not being in tune with tech will jeopardize any efforts to protect proprietary code.

No longer can we afford to humor the attorneys who refuse to accommodate technology. Adoption lags if culture doesn't drive innovation. As in-house counsel, we do not drive innovation. Instead, we are typically pushed, pulled, or dragged along while the company innovates and we try to get the proper agreements and notices in place before calamity strikes.

The workplace is now multigenerational, but the differences between generations are the differences between being digital natives and digital immigrants. Our always-on culture spills over into a profession that was always measured by time and methodical practices. Some of us, at any age, adapt well. Others need intensive training. Adapting will soon no longer be enough; we must be fluent.

In a Legaltech News article, Mark Cohen, CEO of LegalMosaic was quoted:

"Law is now about collaboration of human resources as well as humans and machines. Many still regard tech as a necessary evil rather than a means to the end of providing customer-centric delivery."

Whether serving internal clients or external ones, counsel must be fluent in technology and data practices. Understanding these is as critical as understanding the client's business, product, or service.

Take advantage of available resources (e.g., online communities or peer-sourcing challenges), and use technology to keep your client informed. We have passed the age of periodic updates — we are "always on." We should accommodate in real time.

Author: K Royal is a technology columnist for ACCDocket.com, and director at TrustArc. @heartofprivacy

ACC News

ACC Xchange: The Mid-Year Meeting for Advancing Legal Executives

This reimagined conference (April 28-30, Minneapolis, MN) combines ACC's Mid-Year Meeting and Legal Operations Conference into one powerful event, delivering the trailblazing programs, content, training, and networking you need all in one place, at one time. Register today for cutting-edge mix of advanced-level education at www.acc.com/xchange.

Are you prepared to comply with new state privacy laws?

Rapidly growing data privacy regulations from California to New York make you accountable for all third-party service providers that access, process, or store your company's personal data. Download the case study on Plaza Home Mortgage and the ACC Vendor Risk Service. Visit www.acc.com/VRS for more information.

2019 ACC Europe Conference: Early Rates End 22 March

Join your in-house colleagues from across Europe in Edinburgh 12-14 May for the ACC Europe Annual Conference. This year's theme is *Being a Change Agent in Disruptive Times* and will have three dynamic programme tracks that will give you the opportunity to broaden the skills necessary to succeed in today's legal environment. Early bird rates end 22 March. Register today at www.acceurope2019.com

2019 ACC Annual Meeting: Registration Now Open

Exceptional in-house lawyers make attending the ACC Annual Meeting a priority. Mark your calendars for October 27-30 in Phoenix, AZ for the 2019 world's largest event on in-house counsel. Learn more.

Global General Counsel Summit: London Calling

Are you driving the discussion on corporate sustainability? Positive financial performance, regulatory pressure, material risk, and shareholder expectations are some

continued on page 5

continued from page 4

of the reasons why you should be. Join the critical conversation on "Driving Corporate Sustainability—the Expanding Role of the GC" with your fellow CLOs from around the world, May 22-24, in London, UK. RSVP today.

New to In-house? Are you prepared?

The ACC Corporate Counsel University® (June 26-28, Minneapolis, MN), combines practical fundamentals with career building opportunities, which will help you excel in your in-house role. Come to this unrivaled event to gain valuable insights from experienced in-house counsel, earn CLE/CPD credits (including ethics credits) and build relationships and expand your network of peers. Register at ccu.acc.com.

Drive Success with Business Education for In-house Counsel

To become a trusted advisor for business executives, it's imperative for in-house counsel to understand the business operations of your company. Attend business education courses offered by ACC and the Boston University Questrom School of Business to learn critical business disciplines and earn valuable CLE credits:

- Mini MBA for In-house Counsel, April 8-10, May 7-9 (Los Angeles location), June 3-5, September 9-11, and November 4-6
- Finance and Accounting for In-house Counsel, September 23-25
- Project Management for in-house Law Department, November 13-14

Learn more and register at www.acc.com/businessedu.

Would You Prefer to Call HR or Shall I? Bystander Intervention Training In The #MeToo Era

By Nonnie L. Shivers, Ogletree, Deakins, Nash, Smoak & Stewart, P.C.

"The world will not be destroyed by those who do evil, but by those who watch them without doing anything." – Albert Einstein

Inaction (and complicity by inaction) is a hot compliance topic with nearly all employers. In the #MeToo/#TimesUp era – replete with corporate and individual culpability – two questions have stood out clearly to enforcement agencies like the U.S. Equal Employment Opportunity Commission and should stand out clearly to corporate entities and their counsel. First, ask yourself: have Title VII's and analogous state and local laws' express prohibitions on discrimination and harassment based on sex, race, and other protected characteristics (and retaliation prohibitions for engaging in protected activity related to reports of unlawful discrimination and harassment) effectively eradicated discriminatory animus and retaliatory animus? Have they substantially decreased such alleged conduct in the workplace? To the EEOC, the answer appears simple: no. The effectiveness of Title VII and its comparators in eradicating harassment and discrimination over the past 50 years remains in question. The report issued in 2016 by the EEOC's Select Task Force on The Study of Harassment In The Workplace points the finger at employers, and, in particular, their non-discrimination, non-harassment and non-retaliation training.

There is no doubt training in this space is imperative to set compliance expectations within the culture of the company. While trainings have moved on from corny videos of the lecherous CEO slapping the nubile young assistant on the rump, many trainings have instead devolved into heavy-handed threats of the company being sued to the tune of million dollar judgments (replete with threats of personal liability) by hammering trainees over their heads with black and white examples of what you should NOT do. Do not make racist comments. Do not demand sexual favors for a raise. Do not rescind a job offer due to an applicant's disclosure of pregnancy. The whack-a-mole list of DO NOT DO THIS ostensibly goes on forever and can make trainees feel like they are assumed to be bad actors, bigots and sexists, just like the 1970's era CEO with the bad leisure suit. As counsel, we are intimately acquainted with the panoply of reasons this litany of should not's populates our training modules: nothing is ever dull for an employment lawyer and many schadenfreude-esque mistakes happen.

No doubt, effective training should provide some understanding of the law and how those prohibitions translate into everyday interactions and occurrences in a workplace with realistic, current and nuanced examples specific to the entity. However, the EEOC's Task Force report calls for refocusing and refreshing such hand-slapping training to instead focus on what employees – in particular, supervisory employees – SHOULD DO. A critical part of this equation, at least according to the EEOC, is bystander intervention training. Pause for a moment here. Have you read the report? If not, consider doing so: https://www.eeoc.gov/eeoc/task_force/harassment/. It is admittedly lengthy (at 239 footnotes, it will take you straight back to facing down your law review editor). Said with a straight face as a management-side attorney who sleeps well at night knowing companies are striving for compliance in meaningful ways, the Task Force report is a thoughtful look into what employers can do better to ensure compliance with Title VII's purposes and requirements, no matter what visible or invisible protected characteristics employees may possess, in particular by revisiting basic tenets of professionalism and civility. While recognizing that Title VII and its analogues are not civility codes, most of us would readily agree that incivility and perceived lack of fairness are the gateways to employment charges and lawsuits.

If you read the Task Force's report, you may, like me, find the report short on practical input and solutions as to various recommendations. Bystander Intervention Training is one recommendation. A

continued on page 6

continued from page 5

bystander is anyone who observes a situation (passive bystander) or gets involved (active bystander). The Task Force shares its "belie[f] that bystander intervention training might be effective in the workplace." Why? Because it could create a sense of responsibility with the employee to "do something" and not simply stand by if they are a witness to inappropriate or even harassing, discriminatory, or retaliatory behavior. Because it could give employees the skills and confidence to intervene in some manner when such conduct is observed. Because it could reaffirm for employees the company's stance on "see something, say something" and its culture of compliance in encouraging forthright and timely reporting without fear of retaliation. Even if these suppositions are merely the EEOC's unsubstantiated belief, several states and locales outside of Arizona, including New York City, have amended their EEO laws to require bystander intervention training and access to bystander intervention resources as part of effective anti-harassment training to combat harassment and discrimination.

So how does one train on bystander intervention at various levels? Unfortunately, that is what the EEOC does not share in any meaningful way whatsoever. The report does not contain any substantive recommendations for employers on how to conduct bystander training. The EEOC Training Institute rolled out its own proprietary training and shared its basic outlines for that training, which purport to include bystander intervention training. Former Commissioner Feldblum, however, refused requests that the EEOC share the contents of the EEOC's training, leaving employers to question how to develop and incorporate effective bystander training within their own organizations.

If you are on board with reviewing and potentially expanding your training modules to include bystander intervention training, consider the following practical "how to" tips:

- Introduce and Embrace the Theme: Update existing EEO and/or compliance training for leaders and non-leaders alike to introduce the concept, expectations, and practicalities of "see something, say something" or, put another way, "if someone needs help, help them." It can be as simple as stating that concept in that particular language or the language of your choosing. Whatever way you elect to say it, communicate a sense of responsibility and ownership over the workplace and its culture, thereby creating an ownership mentality. Communicate clearly what the organizational expectation is surrounding an employee's responsibility to "get involved" and where that begins and ends via realistic examples and illustrations.
- Awareness: At its core, bystander intervention requires each individual to be able to identify behavior, language, and actions that fail to conform to company policy and the law, including harassing and discriminatory behavior. Does your training heighten awareness of possible harassment that could happen in your workplace? Does it help employees understand how to deal with an ambiguous situation? Does it aid your employee in critically looking at events and others' reactions to glean what is occurring to the best of their abilities? Is your training specific to your workplace issues and populations, including customers, vendors and other third parties? Does your training cover real issues that could be encountered or have been encountered by similar types of entities? Training modules should contain realistic, modernized examples of issues that cover situations that are not black and white and even topics that feel verboten.
- Build Bystander Intervention Skills: If we expect employees to engage in bystander intervention, employees must know what to do and how to do it. Employers should supply ideas and generate those skills aligned with expectations. Leaders and individual contributors' days will come to confront a difficult situation, if it has not already. Train all employees on real examples of how someone could intervene. Set expectations for leaders that leadership from the top in this area is key. Provide a realistic situation and provide sample responses to interject. Give copious examples of phrasing an intervening bystander might use: "that's not cool, John" or "please stop, Stephanie" or "that strikes me as inappropriate, Sally" or "knock off the jokes about women, Larry!" Supply more than a few ideas, such as direct and less direct approaches: "that's inappropriate, disrespectful, not okay, etc." versus "leave them alone." Give cautionary notes to those who would use humor as an intervention skill, since it can (and often does) backfire and can send the wrong message (e.g., "it's a good thing HR isn't on the phone, Bill!). Warn all employees about the potential effects of failing to act, implicitly condoning the behavior and leaving other employees assuming someone else is addressing the behavior, likely based on seniority or position.
- Reaffirm Non-Retaliation: Employees may fail to act due to fear of potential consequences, stigma, embarrassment, or even retaliation. Employees must know from the top-down that their good faith reports are welcome and encouraged. Leaders must be trained on realistic, granular examples of retaliation, including misconceptions that simply not speaking to or engaging with someone is not potentially retaliatory.
- Incorporate training for leaders (if not all employees) on how to take personal accountability and offer sincere apologies. We all make mistakes and are not sexless, humorless automatons at work. Sometimes even the best and brightest don't bring their best authentic selves to the workplace – that is the human condition. We must all be accountable and atone for our mistakes at times and training on how to confront as a bystander but also take accountability can diffuse situations and de-escalate incivility from a legal claim to an authentic conversation and commitment to do and be better.

Author: Nonnie Shivers is a Shareholder in Ogletree Deakins Phoenix Office. Nonnie partners with employers and managers in three primary ways: litigation avoidance through proactive counseling and training; investigations and resolutions when pre-litigation concerns arise; and litigating legally complex and factually challenging cases to defend employer's actions. nonnie.shivers@ogletree.com

Are You Ready To Sell Your Business? How To Keep The Dream Of Selling Your Business From Becoming A Nightmare

By Jessica Benford Powell & Josh Hencik, Ryley Carlock & Applewhite

Three years ago, you launched your new business. Since then, you have increased revenues every year, hired a dozen employees, outgrown your office space, and built strong relationships with suppliers and customers. Now you are considering selling your business. Maybe you're ready to move onto a new opportunity, maybe you feel you cannot grow the business further on your own, or perhaps you're planning a "someday" long-term exit strategy. Although you may be prepared to sell the business, is the business ready for sale?

Below is important advice on key issues related to preparing your business for sale, so you can get the best value and ensure the transaction goes smoothly.

1. Financial Records Must Be Accurate, Easily Reviewable and Adhere to Sound Accounting Practices to Minimize Risk.

Having a history of accurate, comparable, and easily reviewable financials is one of the most important factors in getting a deal done quickly for a good price. Potential buyers will want at least three years of comparable financials that accurately reflect the business operations so they can confidently value the business.

Most small businesses will not have audited financials, but every business owner should work with an accountant to produce consistently applied financial accounting standards that create accurate and easily reviewable financial records for potential buyers when the business is ready to sell. A selling company with consistent and transparent financials will have a much stronger foundation from which to negotiate a fair price than a company with financials that represent inconsistent and questionable accounting practices, which creates risk for the buyer.

2. Company Records Must Be Current and Accurate to Reduce or Eliminate Future Liability.

Keeping the company's records current and accurate as the business grows is important for all businesses. However, sometimes business owners forget, delay or are not aware that certain company records need to be updated or filed. Before the sale of a business, all company records should be reviewed and updated, government and regulatory filings should be current, and the company should be in good standing. All company policies should be written and all company actions approved and ratified to the date of sale.

All buyers will require a selling company to warrant that its company records are correct and the company is in good standing at the time of the sale. The sellers will usually face perpetual liability for breaching fundamental warranties related to the business organization. Further, all buyers will require documentation that actions taken by the company were properly approved and ratified through the sale, so that the buyer does not face liability from third parties after closing.

One often overlooked aspect of pre-sale diligence is conducting a lien search on the company, and possibly its owners, depending on how the company sale is structured. Business owners should routinely monitor any liens on the company's assets and any liens or pledges against any equity holder's interest in the company, which may affect the ability to sell the company's assets or all of the company's equity in a stock sale.

3. Intellectual Property Assets Should Be Properly Organized, Easy to Access, Registered in the Company's Name and Actively Monitored.

Nearly every business relies on some form of intellectual property as a foundation for its growth and success. Oftentimes a company's intellectual property was designed before the business was formally created, or in its start-up stage, and therefore website registrations, trademarks, and social media may be registered in the names of the company founders. Frequently, as the business grows, intellectual property transfers or assignments to the company are overlooked, only arising when the company is ready to sell and is accounting for the assets it owns.

Buyers will want exclusive rights to all of the business's intellectual property, particularly if the intellectual property is a significant portion of the enterprise value. A seller does not want to delay or lose a deal trying to track down the registered owners of the intellectual property, transfer intellectual property rights to the company, or worse, have to negotiate with a former owner or employee for the rights to intellectual property that were not assigned to the company before the employee left.

In addition, business owners should actively monitor the company's intellectual property throughout the life of the business. Buyers will require sellers to warrant that the intellectual property for sale does not infringe on anyone else's rights and that no third party is infringing on the company's intellectual property rights. Buyers may also require the seller to indemnify the buyer for any issues with intellectual property ownership that may arise after the transaction.

4. Employee Records Must Accurately Reflect Current Rights, Responsibilities, Compensation, Benefits, Equity Ownership and Other Applicable Employment Details.

Another common mistake small businesses or startups make is overlooking the importance of maintaining relevant employee records. Many small business owners, in the flurry of early-stage growth, hire employees and offer raises, equity, and other benefits to key personnel on an ad-hoc basis or without proper documentation. Although companies usually create some form of these employment documents over time, many employees have inconsistent, or non-existent, records regarding hiring, job responsibilities, equity ownership,

continued on page 8

continued from page 7

and benefits. Employee records should be routinely reviewed, particularly before the sale of a business, when a buyer will have to decide whether to retain, terminate or buy-out current employees.

Buyers will review all employment records to understand each employee's rights, salary, bonuses, equity, accelerated payments due upon change of control of the company, potential liabilities under employment and tax laws, such as ERISA, and any other employment matters that may affect the purchase price of the company or liabilities post-sale. The buyer will also want to know if the current employees are under noncompetition and confidentiality agreements which may affect the value of the purchased assets, such as intellectual property, after the sale if the employee is not offered a continuing role with the new owner and is not restricted from using the intellectual property.

Employment issues can be incredibly messy and frustrating for parties negotiating a deal because they have ramifications that touch on labor laws, tax law, and securities laws, among others, and unlike dealing with the transfer of tangible assets, navigating employees through the sale of a company can be a very personal and emotional process. Proper record-keeping not make the change of ownership conversation with employees easier, but it can clearly identify the extent to which each party faces ongoing liabilities if there are issues getting all employees on board with the transaction.

5. Finding the Right Buyer Can Be Critical to Achieving a Smooth Transaction.

When business owners are ready to sell, they may seek out multiple potential buyers and choose the best fit, or a potential buyer may come to the business owner with an unsolicited deal pitch. Regardless of how the potential buyer and business owner connect, it is important for the business owner to be comfortable with the buyer's vision for the transaction and the future of the business. A business owner should not feel pressured into a deal too quickly or without fully understanding the terms of the transaction. The seller should feel comfortable with the buyer's stated objectives and plan for the business after the transaction.

Although the business owner may not be able to control what the buyer does with the business after it is sold, the seller should take the time to find a buyer that shares the same philosophy and business plan as the seller, if it is important to the seller. Also key to the relationship is the business owner's expected role with the company after the sale, which should be clearly identified by the buyer and comfortable to the seller early in the negotiations. The last thing a seller wants is an ongoing contractual relationship with the buyer after a messy and contentious business sale transaction, on terms that were negotiated at the last minute when both parties were experiencing deal-fatigue.

Conclusion: A Long-term Strategy Combined with Proper Legal Representation Goes a Long Way

It is nearly impossible to create an exhaustive list of advice about issues that may arise for the seller of a small business; however, preparing for these major issues far in advance of a sale gives the seller the ability to focus on the transaction instead of distractions.

If you are considering actively shopping your business to potential buyers, or if you simply want to make sure your business is ready if the right buyer comes along, the attorneys at Ryley Carlock & Applewhite are available to assist you in preparing your business for sale and advising you through the transaction process.

Authors:

Jessica Benford Powell helps local entrepreneurs, start-ups, business owners, established companies and financial institutions navigate significant issues related to formation, governance, financing, compliance and intellectual property. jbenford@rcalaw.com.

Josh Hencik is a member of the firm's Corporate and Securities practice. jhencik@rcalaw.com

Patent and Copyright Changes In The New NAFTA

By Michele Washington, Alfredo Solórzano, Roberto Ibarra de Rueda, Jeffrey Morton, Ryan Ricks and Charles Hauff, Snell & Wilmer

Published November 8, 2018 on Law360 (link to original article)

The United States, Mexico and Canada recently reached consensus on the United States-Mexico-Canada Agreement, which is expected to replace the North American Free Trade Agreement in early 2019. Among the numerous topics covered under this modernized trade agreement are several that relate to intellectual property protection and policy.

Some of the more significant updates in the USMCA include provisions relating to copyright term, patent term adjustment, and protection of undisclosed testing or other data for agricultural chemical products, pharmaceutical products, and biologics. Key intellectual property provisions are discussed in more detail below as they impact each of the United States, Mexico and Canada.

United States

Relative to other aspects of the USMCA, the intellectual property provisions found in Chapter 20 of the USMCA do not require the United States to implement many changes at the domestic level. As detailed below, this is not the case for Canada and Mexico, which will have to implement numerous domestic law changes to comply with the USMCA.

continued on page 9

continued from page 8

That said, one area that may result in changes in the United States' domestic intellectual property laws is with respect to moral rights. Moral rights are rights of creators of copyrighted works that are distinct from economic rights.

Under the Berne Convention, moral rights give the author of a work the right to claim authorship of the work and to object to any distortion, modification of, or other derogatory action in relation to the work, which would be prejudicial to the author's honor or reputation. After becoming a member of the Berne Convention in 1989, the United States enacted the Visual Artists Rights Act of 1990, which grants protection to moral rights in visual works only, for example in paintings, sculptures and still photographic images.

NAFTA explicitly stated that no obligation is imposed on the United States in relation to the Berne moral rights provision. However, the USMCA includes no such exception. This may prompt the United States to further develop its moral rights protections. This would provide a more solid avenue for creators of copyright-protected works to control their works and be compensated for them.

Mexico

Unlike the United States, the USMCA will likely give rise to numerous changes in domestic intellectual property laws in Mexico.

For example, with respect to patents, the USMCA incorporates a 12-month grace period for public disclosures originating from the applicant. Mexico currently offers such a grace period, but with certain exceptions which will need to be eliminated. For example, an applicant's foreign patent publication is not currently covered by the grace period. Additionally, Mexico has not previously implemented a patent term adjustment system; however, some patentees have previously been successful in claiming compensation for patent office examination delays (rather than term extension).

Regarding copyright, Mexico will need to implement a notice-and-takedown system for online infringement. However, with respect to copyright term, Mexico already offers protection for life of the author plus 100 years, so no further term extension is anticipated.

Of the three treaty participants, Mexico appears most likely to require significant changes to its domestic intellectual property laws, as the laws and the treaty have numerous inconsistencies. However, the timing and process whereby these inconsistencies will be resolved remains uncertain.

Canada

Like Mexico, the USMCA is expected to have a significant impact on the Canadian intellectual property landscape, including in the areas of copyrights, trademarks, patents and biologics.

On the copyright front, Canada will need to amend its domestic copyright laws so that the copyright term is extended to the life of the author plus 70 years instead of the current life of the author plus 50 years.

On the trademark front, the USMCA requires that a system of pre-established damages be implemented with respect to trademark counterfeiting. This will likely be applauded by law enforcement and brand owners given Canada's checkered past as a haven for counterfeit sales.

On the patent front, Canada will need to implement a patent term adjustment system to compensate patent holders for delay in the issuance of patents of more than five years after filing or three years after a request for examination is made. Currently, Canada has no patent term adjustment system in place.

On the biologics front, the USMCA requires the member countries to provide a data protection term of at least 10 years. Accordingly, Canada will need to extend its current term of eight years to the mandated 10-year term.

Conclusion

The above-described protections should have the effect of improving intellectual property transparency between the member countries, as well as for rights holders and potential rights holders in each nation, and bringing a certain degree of procedural uniformity among the three countries. For example, the USMCA requires that each country ratify or accede to several international agreements including the Patent Law Treaty, Madrid Protocol or Singapore Treaty, and the Hague Agreement. The countries must also establish public online databases for trademarks, domain names and industrial designs, as well as electronic filing systems for trademarks and industrial designs. Additionally, the countries must work with their respective patent offices to share their work, such as search and examination results.

It is expected that the USMCA will be signed before Dec. 1, 2018, followed by ratification in each member country. Once in effect, the USMCA will stimulate a move toward greater harmonization of IP laws across the U.S., Mexico and Canada.

Authors:

Michele Washington focuses her practice on the preparation and prosecution of patent applications in the life sciences. mwashington@swlaw.com

Alfredo Solórzano focuses on real estate and business transactions in Mexico. asolorzano@swlaw.com

Roberto Ibarra de Rueda is an associate in the firm's Los Cabos Office and is in the real estate and commercial finance practice group. ribarra@swlaw.com

Jeffrey Morton is a U.S.- and Canadian-qualified attorney who routinely represents both start-up and large enterprises for their intellectual property, technology and commercial law needs. jmorton@swlaw.com

Ryan Ricks focuses on intellectual property law, including strategic intellectual property counseling, intellectual property transactions, and patent and trademark prosecution, with emphasis on commercialization and licensing. rricks@swlaw.com

Charles Hauff focuses on intellectual property counseling, patent, trademark and copyright prosecution, related litigation and licensing. chauff@swlaw.com

Unknowingly violating non-monetary loan covenants can derail a borrower's ability to exercise conditional ri

A Buyer's Guide for 2019 eDiscovery Tech Investments: Unearthing the True Costs of eDiscovery Technology

Article Provided by Casepoint

In-house counsel and law firms will continue to focus on eDiscovery cost containment in 2019. A new report says that 60% of law departments rate cost control and management as one of their greatest challenges. For many, technology will play a key role in eDiscovery cost management going forward.

It's important for decision makers to understand the business impacts of technology purchases. Before legal teams invest in eDiscovery technology, they'll want to systematically dissect the total cost and efficiency gains of available market alternatives. This white paper explores the cost implications of on-premise solutions and Casepoint eDiscovery. The potential for efficiency impacts are also discussed.

1. Hardware Considerations

eDiscovery hardware costs will be one of the first areas buyers will want to delve into in in their evaluation process.

Layered Hardware Costs

When legal teams go the on-premise route it's important to consider all the costs of installing, managing, and maintaining hardware behind a firewall. Buyers of on-premise solutions spend significant money on servers, systems, networks, and maintenance.

eDiscovery processing and analysis is data-intensive. Large matter data sizes can run in the terabyte range. Thus, the server numbers add up—typically, eDiscovery solutions require 6-12 production servers and 2-3 testing servers. IT spend for database and application servers can run north of hundreds of thousands of dollars upfront. Annual hardware maintenance costs layer on another additional cost each year.

Organizations also need to integrate the eDiscovery solution into their storage, backup, and disaster recovery (DR) systems to ensure sensitive discovery data is always available. DR hardware for eDiscovery runs in the 6-12 unit range. These costs should be added to colocation DR projections for rack size and quantities over time.

A. "Conducting eDiscovery with on-premise solutions requires a much larger capital investment upfront in crucial hardware like servers and backup drives, as well as IT staff to support and maintain the system."

On-premise vs. Cloud Considerations for eDiscovery, ABA Law Technology Today, Sept. 2018

Many legal teams keep eDiscovery data forever, fearing they'll need it in a future legal challenge. At a time when most organizations are trying to get rid of data clogging up servers, on-premise eDiscovery solutions will grow organizations' storage needs and costs significantly overtime.

Buyers will also want to factor in cooling and electrical costs to run on-premise eDiscovery hardware. They may want to account for some portion of server room real estate costs too.

Erase eDiscovery Hardware Costs

The Casepoint eDiscovery solution is cloud-based. There are no hardware or maintenance costs. Organizations will also save on utility costs. Casepoint takes care of all utility costs for the servers that run the eDiscovery software.

Conducting e-discovery with on-premise solutions requires a much larger capital investment upfront in crucial hardware like servers and backup drives, as well as IT staff to support and maintain the system.

2. Software Elements

Buyers will want to avoid eDiscovery software that is one big, pricey, unruly, licensing-gorilla.

Unruly, Hidden Licensing Costs

Many eDiscovery software tools are on-premise and single-purpose. Purchasers can buy separate products for legal hold, collection, early case assessment, review and production. Most of these vendors charge additional fees for analytics, machine learning, user fees and other add on charges. With this approach licensing is unpredictable and expensive.

Buyers that go in this direction will encounter a morass of licensing fees. They will want to look under the hood during the sales process and ask about licensing costs for all eDiscovery stages. Is there a base fee and a per seat/user fee? Are advanced tools like AI included in the software license? Also, some vendors charge extra for the analytics legal organizations will want for managing eDiscovery from a business perspective.

Getting an organization's arms around this licensing gorilla is a huge, ongoing chore. They end up paying for and managing multiple licenses for different purposes. Licensing can break down as:

- Collection software
- Processing software
- Review software
- Artificial intelligence software
- Analytics software
- Production software

Supporting Jungle of Software

It's important that buyers not underestimate the costs of supporting software necessary to run separate, on-premise eDiscovery tools. With the gorilla approach, organizations end up with a jungle of additional licensing costs, renewals, and care.

On-premise products require SQL server software licenses and management. Decision makers will also want to calculate enterprise operating software prorated costs into the total cost equation. Annual enterprise software maintenance fees should not be overlooked either. Vendors typically charge 20% of the software cost.

The bottom line: enterprise SQL and operating server licenses complicate and expand the total cost of eDiscovery.

continued on page 11

continued from page 10

eDiscovery Software Updates

On-premise eDiscovery applications must be periodically updated under pricey maintenance agreements. Keeping all the single-purpose software: collection, processing, review, analytics--up-to-date is like a jungle that must be constantly tended with a machete. Buyers should plan on paying a pretty penny to keep eDiscovery teams working on the latest, optimized software version.

B. "For the last 2 years more than 25% of law firm IT leaders ranked keeping up with software changes as one of their top 3 issues/ annoyances."

ILTA 2018 Technology Survey

Uncomplicate Software Costs

Casepoint is designed for simplicity. Organizations pay one fee for collection through production. The single price encompasses the application, servers, server software, hardware, and automated application updates. Cost simplicity and transparency help buyers avoid surprise, extra fees not accounted for in total cost estimates.

With Casepoint organizations get:

- One technology fee for everything
- No server software costs
- No eDiscovery software maintenance fees
- No pro-rata enterprise server software or maintenance costs

3. Resource Burdens

Buyers investigating the total cost of eDiscovery technology alternatives often overlook the resource burdens. It's important to delve into the staffing requirements for managing, maintaining and using the technology before making a purchase.

Multiplying Personnel Costs

On-premise eDiscovery hardware and software requires IT resources for management, security, maintenance, and updates activities. With this approach organizations end up paying for multiple staffing layers. Litigation support folks manage data ingestion, processing and the like. IT experts take care of collections, servers, backup, and DR system management. Buyers need to calculate these personnel costs into total cost estimates.

There is a new trend of law firms starting to track IT operating costs per attorney. Because all legal teams rely on electronic data to find and analyze facts and strategies, eDiscovery software has become a fundamental tool for practicing law. Organizations that choose on-premise eDiscovery solutions with multiplying IT personnel costs will watch this telling cost metric grow rather than shrink overtime.

C. "20% of law firm are tracking IT operating costs per attorney"

ILTA 2018 Technology Survey

Efficient Resource Allocation

Buyers bent on minimizing eDiscovery personnel cost burdens will want to consider Casepoint. Legal technology experts manage all application and server software at no extra cost.The software is so intuitive that litigation support folks typically execute collections, even for cloud sources.This team also manages user access controls.There is no personnel burden for managing a jungle of software updates—users simply go to a secure portal where the most current version is always available.

4. Efficiency Across the Organization

When selecting eDiscovery technology, buyers need to evaluate efficiency gains that will accrue to the organization, departments, and users. eDiscovery data sets are massive and deadlines extremely tight. Given this, organizations want a solution that provides infrastructure speed, software usability, and mobile workforce access.

Litigation Need for Speed

Shared IT infrastructure in organizations with on-premise solutions frequently slows down eDiscovery collections and processing. Sometimes there just aren't enough servers available to efficiently handle a new massive data set. When litigation support lacks the compute power for rapid data loading, processing, indexing, and review, then big delays happen. Early case assessment is at a standstill until the lawyers get their hands on the prepared data.

With Casepoint server capacity, litigation support teams can get data ready in hours or minutes rather than days or weeks. Built-in quality control steps minimize mistakes that require re-dos. Teams can say goodbye to internal IT resource-hogs slowing down litigation support.

D. "Many IT departments still operate their eDiscovery infrastructure on the same oversubscribed hardware that is used for regular infrastructure, causing performance issues …"

On-premise vs. Cloud Considerations for eDiscovery, ABA Law Technology Today, Sept. 2018

Accelerate Attorney Productivity

Lawyers and paralegals also excel when freed from the constraints of internal shared IT infrastructure. When reviewing masses of data, processing speed is paramount. With Casepoint, lawyers no longer drum their fingers while waiting for documents to appear after a search. Mobile lawyers can easily and securely upload "hot documents" to share with colleagues, co-counsel, or clients. Access to high speed review and analysis technology via a portal, also eliminates delays from common VPN access problems or servers choking on large data sets.

Organizational Benefits

Casepoint gives organizations massive compute power without the on-premise solution costs and resource burdens. Hundreds of Casepoint servers empower teams to rapidly analyze large data sets for faster, informed, fight-or-settle decisions. Executive-level analytics and dashboards help general counsel or the partner-in-charge manage litigation and investigation portfolios from a business perspective.

Organizations can also attack all the duplication of effort in eDiscovery. Casepoint makes it easy for legal teams to reuse attorney work product across matters. For example, documents tagged privileged in one matter don't need to be re-reviewed

continued on page 12

continued from page 11

for privilege again in the next matter. Technology that automates reuse of tags across matters will save organizations tons of review time and costs. Imagine the total eDiscovery cost savings in organizations that leverage work product reuse across their portfolio.

5. The Buyer's Journey

Buyers mulling over eDiscovery technology investments in 2019 and beyond will want to weigh the factors discussed in this paper. Tallying up the full hardware, software, and resource costs of on-premise solutions is critical for wise investments. Decision makers should also evaluate efficiency gains from technology alternatives for all stakeholders and the organization as a whole. With continuing pressures to "run more like a business" law departments and law firms alike need to dissect the true costs of eDiscovery technology to make good business decisions.

Organizations can learn more here about the eDiscovery total cost advantages of Casepoint.

For more information, please contact Paul McIlroy (pmcilroy@casepoint.com) at Casepoint.

The Arizona Chapter gratefully acknowledges the support of our 2018–2019 Newsletter Patron

casepoint

Chapter Leadership