EMPLOYMENT AND ECONOMIC DEVELOPMENT

Lathrop GPM

A Legal Guide To TECHNOLOGY TRANSACTIONS

A COVID-19 Update

2020

A Collaborative Effort

Minnesota Department of Employment and Economic Development

Lathrop GPM

A Legal Guide To
TECHNOLOGY TRANSACTIONS

A COVID-19 Update 2020

is available for viewing and download from the Minnesota Department of Employment and Economic Development (DEED), Small Business Assistance Office.

Office address: Great Northern Building, 12th Floor, 180 East 5th Street, St. Paul, MN 55101-1678.

Telephone: 651-556-8425 or 800-310-8323
Fax: 651-296-5287 | Email: deed.mnsbao@state.mn.us
Website: Small Business Assistance Office

This guide is also available from Lathrop GPM, 500 IDS Center, 80 South Eighth Street, Minneapolis, MN 55402
Telephone: 612-632-3000
Website: Lathrop GPM

Upon request, this publication can be made available in alternative formats by contacting 651-259-7476.

A Legal Guide To
TECHNOLOGY TRANSACTIONS
A COVID-19 Update

2020

Primary Author: Michael R. Cohen
CIPP/US, CIPP/E

A Collaborative Effort

Minnesota Department of Employment and Economic Development
Lathrop GPM

ISBN 1-888404-82-4

TABLE OF CONTENTS

PREFACE

The acquisition of information technology is a major event for any business since it affects operations, management, and ultimate profitability throughout the business' supply chains and production processes. The issues associated with such an acquisition can be complicated and complex and should not be left to chance but instead addressed directly in any contracting for the information technology.

Lathrop GPM and the Small Business Assistance Office are pleased to present this brief primer on the subject to better enable businesses considering information technology acquisition to frame up their questions and issues for their own staff, for technology suppliers, and for consultants and attorneys who will be involved in the contracting, acquisition, and use of the technology.

A special note of thanks to Lathrop GPM lawyer Michael Cohen for preparing these materials.

Charles A. Schaffer
Director, Small Business Assistance Office
Minnesota Department of Employment & Economic Development

2020

DISCLAIMER

This Guide is designed to alert businesses to legal issues which commonly arise when acquiring technology. It should only be used as a guide and not as a definitive source to answer your legal or business questions. The materials in this Guide are intended to provide general information and should not be relied upon for specific legal advice. Legal and other professional counsel should be consulted. Lathrop GPM and the Small Business Assistance Office cannot and do not assume responsibility for decisions based upon the information provided in this Guide.

INTRODUCTION

The Coronavirus (COVID-19) outbreak has required businesses to develop contingency plans to handle the disruptions it has caused and will continue to cause.

The devastating impact of the COVID-19 pandemic has included a profound movement of businesses to create flexible digital workplaces, remote working, and e-commerce platforms to help employees better serve customers, distribute products, and ensure business continuity.

Maintaining supply chain resilience has become vital to business success. Businesses would be wise to leverage platforms that offer applied analytics, artificial intelligence and machine learning to maximize efficiency and still ensure end-to-end transparency.

Cybersecurity and privacy, new regulatory obligations, business continuity planning, and related issues must now be a focus of any technology transaction.

While businesses move quickly to adapt to the structural changes brought on by the pandemic they must still consider how such changes will be implemented and remain in effect once the virus has been defeated.

The expansion of remote workplaces may also increase potential vulnerabilities to cyber-attacks such as phishing and other efforts by hackers to access valuable information. Businesses must establish clear rules and guidance for those working remotely, using a virtual private network (VPN) for network access,

multi-factor authentication (MFA), mobile device management for connected devices, encryption as possible and feasible, regular patching of software, and limiting access to a need-to-know basis.

When looking at various technology solutions, a business should remain mindful of the legal issues that are common in technology related agreements.

While many of the suggestions in this Guide assume time to plan and test is available we recognize that the COVID-19 pandemic has forced some prompt decision-making without the luxury of time or planning. Hopefully this Guide will still offer tips and guidance to those looking at the requisite technology agreements.

In the words of Aristotle -

"How many disputes could have been deflated into a single paragraph if the disputants had dared to define their terms?"

Information Technology -A Key Asset

Few businesses or organizations can survive today without efficient and effective information technology, and a business disruption caused by a pandemic, failed system or a data breach can be devastating. From basic word processing to sales force automation and electronic health records, financial reporting, product manufacturing and delivery, the use of technology to receive, store, manage, record and transmit information has become essential to virtually every business and organizational activity. The increasing use of mobile applications, cloud based technologies, connected devices and the internet of things, artificial intelligence, and the rapidly increasing data breach rates have added new issues to consider when managing personal and business information.

The use of blockchain and cryptocurrency in sales and supply channels has added new benefits and complexities to the use of technology in contracting. So-called "smart contracts" allow computers to buy, sell, and supply products between two parties without any human intervention.

Whether a hospital or clinic providing mission critical patient care, a franchisor or franchisee operating sub shops, or a designer, importer and distributor of giftware, your business could not likely survive without the software applications and processes used for supply chain management, inventory control, human resources, financial management, accounting, e-commerce, legal compliance and other key business functions.

When the technology works everyone is happy. When the system crashes a business or organization can easily become crippled and the following questions will soon be asked:

- *How quickly will the problem be fixed?*
- *Who is responsible and how will we get the system back in operation?*
- *What alternatives are available?*
- *What remedies or recourse do we have under our agreements?*
- *What costs or damages are we likely to incur?*
- *How can we avoid this happening again?*

If you are the CFO, CEO, or other person responsible for selecting the technology or systems used to run your business or organization, your ability to sleep well at night may depend on whether your systems or technology will meet all of your business or organization's functional needs and requirements. To access your company's technology investments, you may wonder:

- *Will management and shareholders feel confident that the expenditure was a wise investment?*

- *Will your business or organization be at risk for any failure to comply with federal or state laws because the computer system or technology is inadequate to meet fundamental recording and reporting requirements?*

- *Is the system going to mitigate or increase potential risk and liability?*

The purpose of this Guide is to identify some of the key issues and concerns that any business or organization should consider when acquiring computer systems or related technology. It should help you to more efficiently plan for the procurement of technology and the use of appropriate contracts and agreements that can help avoid some of the painful lessons learned by others who have experienced failed systems or technology projects.

While a well drafted written agreement is no substitute for a fully functional and secure system, the agreement itself can serve as a useful management tool to document the needs and obligations of both parties.

We hope that this Guide will allow anyone involved in technology transactions to form a basic understanding of what issues are important and merit further discussion with legal and other professional counsel.

To facilitate revisions or updates of this Guide, this publication is available on Lathrop GPM's website at https://www.lathropgpm.com/ as well as the website of the Minnesota Department of Employment and Economic Development at https://mn.gov/deed/. If you are looking for the most current version of the Guide, please check the above websites to see if an update has been completed. It is our sincere hope that you will find the following Guide helpful as you seek to achieve agreements that are a "win win" for both parties.

Michael R. Cohen, CIPP/US, CIPP/E
Lathrop GPM

CASE STUDY: AN ERP SYSTEM GONE BAD

The following is a true story. A designer, importer, and distributor of collectible giftware with annual revenues of $250 million hired a consulting firm to oversee the selection and implementation of an Enterprise Resource Planning (ERP) computer system. When the new system was being installed, the consulting firm estimated the cost to implement the system at $3 million. The cost after implementation was over $12 million. When the new system was finally put into operation, the business was so totally disrupted that it was virtually destroyed. Orders could not be taken, or if taken, were irretrievably lost. Orders were not properly filled and shipments went out with no billing. The business spent millions of dollars in an attempt to remedy the problems and in the process lost significant goodwill and continued patronage of a great number of its customers.

Many lessons can be learned from this failed implementation.

USE DETAILED SPECIFICATIONS AND RFP/PROPOSAL FOR VENDOR SELECTION

Why is this system being purchased, what components are sufficient, and what service levels are necessary?

It is important to first analyze the particular needs of your business, the capabilities and capacities required of the contemplated system, and the ability of a proposed system to fulfill those needs. Take time to prepare a detailed written statement of the functions and performance you expect from the new system. These requirements and specifications can be written either by your own staff or by an independent consultant. Once you have documented your specific needs you can prepare a Request for Proposal (RFP) with sufficient detail to solicit vendors. These requirements and specifications can then be made part of any final written agreement.

You might assume in acquiring technology that it will perform just as it was demonstrated or tested. You might also assume that it will certainly meet your specific needs. Do not count on the technology vendor to guarantee such performance. Forget about all those wonderful statements, whether oral or in writing, made by the sales representatives and others who are anxious for you to acquire their system or the latest and greatest technology solution. In fact, the vendor's standard contract will most likely specifically disclaim any warranties and state that any promises or assurances made by the sales representatives or others, even in writing, are not valid or enforceable.

The following is a merger or integration clause that typically appears near the end of most agreements:

> "This agreement sets forth the entire understanding between the parties and supersedes any prior representations, statements, proposals, negotiations, discussions, understandings, or agreements regarding the same subject matter."

Because this clause knocks out all previous agreements or understandings between the parties, it is essential to incorporate by reference in any final agreement the RFP, the vendor's proposal and response to the RFP, as well as any other significant and relevant documentation that you relied upon to acquire the technology or system. If you are relying upon any verbal assurances, make sure that they are memorialized in writing and identified as part of the final agreement.

Even when you are creating the initial RFP for the purpose of soliciting vendors you should be thinking about what express warranties should be included in the final agreement with the selected vendor. You might even ask the vendors to submit their proposed agreement so that you can review it as part of the selection process.

PERFORM ACCEPTANCE TESTING

Even if the system you are installing or the technology solution you are considering has been around for years and is primarily off the shelf software, or proprietary technology that is not highly customized, you should still have a process that allows you to test the functions and features of the system or technology within a reasonable period of time necessary to determine whether or not it is acceptable. This test should be performed using real data in your environment and completed before you go live with full scale implementation of the system.

The only way to assure successful implementation of a system is to clearly set forth an evaluation and testing process that is mutually agreed upon by both parties. By using mutually agreed upon functional requirements you can establish acceptance criteria that will prove beneficial to both parties. Through this evaluation and testing process you will be able to determine that the system performs in accordance with your requirements. This process will also allow the vendor to identify and understand what it needs to accomplish to achieve delivery and acceptance of a satisfactory system or technology. This way there will be no surprises and both parties will understand their obligations.

The acceptance testing provisions should cover (1) pre-live and post live testing, (2) duration of the test and any retests, (3) rejection of the system if necessary, and (4) remedies for failure to meet acceptance testing criteria and milestones. In some cases payments can be tied to successful completion of acceptance testing.

Purchasing technology to run a business is not the same as buying furniture or other large scale purchases where the buyer can usually determine at the time of delivery whether or not the items purchased were what they ordered. Acceptance testing is one of the unique features of information technology agreements and may be appropriate for your transaction.

INCLUDE APPROPRIATE EXPRESS WARANTIES

Standard vendor agreements will likely disclaim all ***implied*** warranties, including any warranty that the technology or system will be suitable for any particular purpose. Vendors will not want to assume such open ended risk and liability. These disclaimers of ***implied warranties*** are permitted under the Uniform Commercial Code and appear in virtually every software related agreement. It is unlikely that you will be able to negotiate these standard disclaimers out of the agreement. It is essential, therefore, to have relevant and appropriate ***express*** warranties stated in the agreement. For example, the vendor should expressly warrant that the system or technology will conform to and perform in accordance with the functional requirements and specifications set forth in an exhibit to the agreement or as contained in the RFP and the vendor's proposal. If possible you should also review any relevant specifications and documentation referred to in the agreement to make sure it is appropriate and sufficient.

Additional warranties set forth in the agreement might require a prompt response time, limited down time, sufficient capacity or other performance features. If the system must generate timely reports, you should make sure that these requirements are clearly identified. If your business is concerned about compliance with certain federal and state laws and other special needs, you should make sure that you identify appropriate warranties of performance as part of the agreement.

The process of negotiating express warranties can prove invaluable in analyzing potential risks and concerns. If these issues are identified early in the procurement process, they can be more easily and less expensively resolved. The vendors' reluctance to provide reasonable warranty protection might also be an indicator of the vendor's own lack of confidence in the technology as a solution to the needs of the business.

Appropriate system testing coupled with express warranties of performance prepared in accordance with mutually agreed upon specifications would be protective of both the buyer and the purchaser and may help avoid arguments over failed systems and any resulting litigation.

Here are examples of express warranties to consider if appropriate for your transaction:

Ownership. Warranty that licensor is the owner of or has the right to grant a license to use the system without violating any third party rights.

Performance. Warranty that system will conform to and perform in accordance with specifications.

Response Time. Warranty that system will have sufficient response times for transactions and sufficient response time to any technological failure of the system.

Capacity. Warranty regarding the bandwidth of the system for maintaining records, files, and other data and achieving any agreed upon service levels or response times.

Compatibility. Warranty that system acquired will be fully compatible and integrated with the user's hardware and software environment.

No Viruses. Warranty that the system contains no undocumented features, viruses, or drop dead devices.

Documentation. Warranty that documentation is adequate and is sufficiently detailed, complete, and accurate.

Current. Warranty that the software will be updated and kept current as necessary to comply with any changes in federal or state laws and regulations.

Complete. Warranty that the system includes all necessary hardware and software necessary to conform and perform in accordance with specifications and no additional hardware or software is required.

NEGOTIATE RELEVANT DELIVERY SCHEDULES/MILESTONES

You can quickly lose control over the costs of a large-scale system implementation project, especially if the work is paid for on a time and materials basis and not a fixed bid project. Performance milestones can help establish checkpoints to ensure progress towards a successful implementation and allow both parties to monitor progress and address problems early in the implementation. It is important to maintain a good relationship between the technology vendor and the information technology personnel who are employees of the business or organization acquiring the technology. It is however also important to make sure that the vendor personnel are held accountable for their performance and those managing the project can assert relevant controls. The business should be willing and able to continuously question the performance or resulting deliverable and not wait until too many problems escalate and too much money is spent. Letting problems and issues remain and escalate in a software implementation is a recipe for disaster and litigation.

Finally, it may be helpful to consider how the contract will be used as a tool to manage activities after it has been signed. The agreement can be more than just a means to enforce specific remedies or pursue litigation.

NEGOTIATE PROGRESSIVE PAYMENT SCHEDULE

As payment terms often dictate deliverables and provide a chance for parties to evaluate their progress, setting out these terms clearly can save hassle and side-step unmet expectations. Some important questions to consider:

- *How are payments made, and when?*
- *Fixed lump sum?*
- *Fixed periodic fee?*
- *Time and materials or other variable?*
- *Is payment based on performance?*
- *Upon execution of contract?*
- *Upon delivery or installation?*
- *Completion of training?*
- *Upon completion of acceptance testing?*
- *Upon productive use or when system goes live?*
- *Specified number of days after any one of the preceding events?*

What is included in the fees paid?

It is critical to specify what is included such as hardware, software (including third party software), custom modifications, updates, enhancements, new releases, documentation, delivery, installation, training, support, maintenance, technical assistance, disaster recovery, warranty, taxes, travel and other expenses.

When listing deliverables it is important to be precise in what you are getting for the fee paid. For example, if you are paying for support that includes "upgrades" or "enhancements," how are they distinguished from new products that are sold for additional license fees is an important component in evaluating pricing.

Vendors will expect to be paid an amount that at a minimum can cover their personnel costs, especially if extensive services are necessary to implement the project. Starving a vendor of cash will not guarantee quality performance. People need to and expect to get paid.

The purchaser or licensee will most likely seek some form of acceptance testing that can be linked to a payment schedule. They may, however, find resistance from a vendor that is a public company and is required to follow accounting rules concerning revenue recognition. While being sensitive to revenue recognition rules and the vendor desire for early payments, it is still appropriate for any business buying technology to use payment as a motivation for performance and completion of the system. By withholding a portion of the fees until final completion or linking payments to the achievement of critical milestones, the purchaser can provide a strong incentive for the vendor to complete the performance in a timely fashion and in accordance with the customer's requirements.

A reasonable amount of the purchase price or license fee might be withheld until after the system is fully operational, tested and accepted to assure that it meets all of the customer's functional needs and requirements. Progressive payment schedules can be tied to critical events with the length and degree of acceptance testing negotiated with the vendor so that it is fair to both parties. This approach allows the buyer to have some comfort that all critical business functions are met before a final payment is made. It also removes any doubt for the vendor that it is on track to complete the project without any disputes or challenges from the customer.

BE CAUTIOUS WITH FIRST TO TRY-ALPHA/BETA TEST

Your business or organization might benefit from being the first to try a new technology or system, and being the first might provide a competitive advantage. There might also be a steep discount available for being the first business to try some untested technology. The vendor may be looking for a business willing to take some risk and be the pioneer. By testing the new technology or system through an alpha or beta test you will provide important data to the vendor so that they can improve upon the application or correct any defects or problems with the technology. In exchange for sharing this information and acting as a "guinea pig" you might receive a reduced license fee or other consideration. Your business might even benefit by having the technology developed with your specific needs and requirements in mind.

There are, however, obvious drawbacks to being the first or early adopter and user of any technology. Reliance upon a technology that has not yet been fully tested and proven to work in your business can result in unforeseen problems and delays in implementation. Most businesses do not have the luxury to risk their key business operations to such experimentation. For that reason, you should make sure that any significant system implementation or technology acquisition has been fully tested before it is used in your real operations using real data for a significant period of time and for a significant number of customers. References of similarly situated customers should of course always be checked to assure vendor credibility. If you are participating in such an alpha or beta test you will likely be asked to sign an agreement that requires you to keep

the results of the test confidential and imposes other requirements on your participation. It would be appropriate to include the form of consideration you receive for such participation, including any free or reduced licensed fees. The vendor might also limit your use for non-productive testing purposes unless and until a fully tested version is complete and ready for commercial distribution.

CONSIDER RESPONSIBILITIES FOR SYSTEM REPLACEMENT AND CONVERSION

Is the conversion process from the old system to the new one your responsibility or the responsibility of the vendor?

If a legacy system is being replaced there may be additional time and effort necessary to maintain the legacy system for a period of time until a cut over to the new system is appropriate. This cut over and transition from one system to another should be considered in the agreement. The feasibility of how, and specific manner in which your existing procedures and information will be transferred from manual or automated systems to any new replacement system and at what cost are important considerations. You should have a clear understanding of precisely how and when this conversion will be done and by whom. The time and expense involved in a conversion process to new technology is frequently overlooked and should be considered when preparing the key milestones to include in the final agreement. It might be appropriate for example to have parallel systems operating for a limited period of time or at least until the new system proves that it can operate successfully.

DEFINE DISASTER RECOVERY PROCESS, POLICY, AND PROCEDURES

Disaster recovery includes the process, policies, and procedures a business has in place for the recovery or continuation of the technology infrastructure necessary for the ongoing operation of the business. Every business should have a disaster recovery plan and be sure that the agreements in place with technology vendors supports the plan.

When working with any new vendor, it is important to understand what backup systems or disaster recovery options are available and at what additional cost. If appropriate, these options should be covered in the agreement. Disaster recovery services usually offer a type of temporary working environment if yours is disrupted. Applications and data might be hosted in an alternative data center, which is connected to your network, and made available during the disaster. Note that it is not uncommon for vendors to subcontract out disaster recovery obligations, and many other third parties are often involved (the provider of the alternative data center, the provider of the original data center, a network service provider).

Typical disaster recovery provisions include representations that the vendor will maintain (or cause to be maintained) backups of certain content, and employ disaster avoidance and recovery procedures in accordance with “standard industry practices.” Instead of invoking so-called standard industry practices you might request more details as to what practices the vendor actually allows and what other third-parties the vendor may subcontract with in

the event recovery efforts are extensive. You should consider what access rights you have to any facility used for disaster recovery and the ability to do a test of the disaster recovery in action. You might also allow for periodic testing, and the maintenance by vendor of certain levels of power supply and equipment.

What constitutes a "disaster" for purposes of triggering the disaster recovery services provided by the vendor?

When defining the term and triggering events make sure that it is not too limited. Would a pandemic like COVID-19 be covered? If a list of disasters are identified you might consider adding the statement "including but not limited to." A vendor might also want to have the disaster recovery services limited in duration. It is critical however that the "alternative system" remain available until your disrupted system is once again live and capable of running the key business functions. While you are not likely to invoke such a disaster recovery plan unless absolutely necessary you need the assurance that when invoked you will not be arguing with a vendor over whether or not a "disaster" has occurred. Common issues in negotiating disaster recovery include response times (between when the determination a "disaster" has occurred is made and when the back-up plan is working), service levels during the disaster period (are you comfortable with these being reduced during the disaster?), and any force majeure provisions (these need to be considered carefully since the occurrence of an event beyond the parties' control is precisely what disaster recovery plans are meant to cover).

Does the vendor use the cloud as a back-up or disaster recovery tool?

The cloud (see discussion below) has become an increasingly popular method of providing disaster recovery services. When considering the cloud as an option make sure that you consider issues such as data privacy and security and other issues related to doing business in the cloud. Whether using the cloud or a remote facility for disaster recovery, make sure that the technology agreements that you have in place with various vendors allows for such outsourcing. You do not want to find that your disaster recovery plan when implemented results in a breach of one of your license agreements with a software provider that had limited your use to "one copy installed on one specific server." This may require a review and possible revision of licenses to clarify such use for disaster recovery purposes.

IDENTIFY KEY PERSONNEL

Have you met the vendor employees assigned to manage your account once the agreement is in place?

When considering a technology solution or vendor, the buyer is typically persuaded not just by the technology itself but the people who they meet during the sales process. Vendors are most attentive and responsive before the agreement is signed and the deal consummated. During this courtship period, the vendor introduces their best and brightest employees. While these individuals may primarily be sales people, it may be appropriate to interview the specific employees who may play a key role in the system implementation or any related consulting services. This is especially true if these individuals will be working at the business location or have substantial interaction with your staff. If there are any vendor employees that are particularly critical to the success of the project, the business might consider including a key personnel provision in the agreement identifying such individuals. Simply because you meet a remarkable and talented person during the sales and vendor selection process there is no assurance that you will ever see or hear from them again after the agreement is signed unless they are identified as a key person in the agreement. From the vendor's perspective they will want some assurance that they can assign and staff the project as appropriate and use their "star" employees for multiple projects.

Vendors may also be concerned about losing employees that they have invested significant time and money to train and will add a non-solicitation/no-hire provision in their agreements. Make sure that this proviso is reasonable and reciprocal so that you do not lose any key information technology employees to the vendor.

UNDERSTAND USE OF HOSTING, SUBSCRIPTIONS SERVICES, APPLICATION SERVICE PROVIDER (ASP), SOFTWARE AS A SERVICE (SAAS), AND THE CLOUD

Information technology is available in a number of different forms so that businesses now have a variety of options to consider. One of the fastest growing areas of technology licensing and acquisition for businesses is the use of hosting, subscription services, ASP, SAAS, and the so-called cloud. Today, almost any IT resource can be delivered to a business as a cloud service, from proprietary databases and software applications to network configuration.

Remote workplaces and the use of e-commerce will likely remain a more common way of doing business following the massive and widespread transition to these workspaces and platforms resulting from the COVID-19 pandemic.

Many businesses have already come to rely on these remote access computing services to run business applications without a large investment in new servers or other hardware. These cost saving measures can be attractive but require special scrutiny as new legal issues arise as a result of these new methods of technology delivery. As noted above, the cloud has become a popular and economical way to provide disaster recovery services.

Given that cloud service providers use the internet or a private network to deliver their services, businesses are exposed to data loss and services outages. One way to minimize risk of network failure is to engage with multiple cloud service providers. However, businesses may find a multiple vendor solution impractical because of a lack of interoperability between cloud service providers.

Businesses can also mitigate the risk of system outages and data loss by carefully reviewing a cloud service provider's infrastructure, with a focus on their business continuity procedures (BCP). A cloud service provider should attach a written BCP to any agreement to render services. To further minimize risk, a customer should require a contractual right to review and approve changes to the BCP.

Another key issue to address is whether the vendor is sub-contracting any of its services and/or placing any restrictions on its own liability for system failures (for example, a vendor may state in its agreement that they "own or license" the services they provide). Many cloud customers may be surprised that cloud service vendors frequently use sub-contractors to expand their own clouds. You should make sure that any sub-contractors involved have the same quality of service as the vendor, and that the vendor does not remove itself from liability for acts or omissions of its sub-contractors.

You may also want to address the transferability of these services from one provider to another, should you wish to transition to a different vendor. Make sure that your data is not held hostage by a vendor and can be easily transitioned to another vendor.

Provisions for maintaining the data in certain formats and time lines in the case of a requested transfer should be established. How to track and audit data stored in the "cloud" also presents a legal and regulatory issue. A services agreement should stipulate that the vendor is able to keep track of the information it holds in a manner sufficient for your needs (e.g. if litigation is anticipated, it may be necessary to perform "record holds" or establish an audit trail).

Does the cloud arrangement address data privacy and security issues?

One of the major concerns when using the cloud or other outsourcing is data privacy and security. Customers desire not only to protect their company's most valuable information, but to comply with the multitude of state, federal, and even international laws that apply to businesses that store any type of "personally identifiable information." These laws can require the encryption of, restriction of access to, and deletion after certain time periods of data, the notification of a breach to customers whose data privacy is compromised, and even the explicit use of contractual provisions with service providers surrounding privacy and security safeguards. It is important to recognize which laws apply to you (for example, certain laws apply only to specific industries such as health care or banking; other laws are particularly strict in certain geographic areas, such as California, Massachusetts, and the European Union).

When reviewing the vendor agreement, consider what physical and information security is employed by the vendor. The jurisdiction in which the data is stored may implicate certain laws so you should either identify and limit where the servers can be located or make sure that you understand and can comply with the necessary laws.

You should carefully review the vendor's security measures and contractual commitments. Since vendors store data from multiple customers, you should consider conditions on their use of your data for aggregation or cross-tabulation purposes. For example, you might include provisions prohibiting the vendor's use of your data for purposes other than providing direct services and defining such data as your "confidential information". You should also make sure that any use of data that involves personally identifiable information not only complies with all relevant federal and state privacy laws and regulations but is also consistent with your own privacy policies and data security procedures.

THE INTERNET OF THINGS (IOT) AND ARTIFICIAL INTELLIGENCE (AI)

One of the fastest growing areas of new technology is known as the Internet of Things (IoT). The IoT is the expanding network of interconnected "smart" consumer products, ranging from Amazon's Echo to "smart home" products that control temperature, lighting, and even home security. While IoT devices can streamline a business's functions in a myriad of ways, there are several key issues to keep in mind when considering acquiring IoT technology.

We live in a world where phones, cars, clocks, kitchen devices, appliances, and other household products monitor consumer behavior and communicate with us and each other via the internet. The collection of data by these devices presents enormous opportunities for businesses to gain efficiency, improve quality, decrease costs, and improve performance in products and services. IoT encompasses the ability of such devices and systems to connect wirelessly and the increasing number of products created and sold that allow for such connectivity. These internet connected devices are enabled by small embedded computer processors and software. In the narrowest definition the IoT involves connecting electronic devices to the public Internet. Just as there is no widely accepted definition of IoT there are likewise no uniformly recognized IoT standards for communication or security protocols.

It is estimated that the number of internet connected devices is well over 17 billion, more than 2 per person on the planet, and will likely double in number by 2025. IoT applications are projected to produce over a trillion dollars in value for businesses.

While such connectivity offers enhanced efficiency there is concern that with the fast growing IoT market, little attention has been given by manufacturers to data security which is often treated as an afterthought to innovation and other features for the so-called "smart" technology. IoT devices may therefore be delivered to consumers with well- known security vulnerabilities that could have been corrected in product development and prior to shipment.

With the proliferation of these smart devices come legal concerns. Automobiles, medical devices, including pacemakers and insulin pumps may be vulnerable to cyber-attacks. When these devices are hacked they can be converted into a massive network of remotely controlled machines known as a botnet with severe consequences to hundreds of thousands of consumers.

As more and more personal information is collected and stored by these devices they are becoming an increasingly popular target for hackers. Businesses that manufacture and sell IoT devices, as well as owners of networks, and consumers must consider what roles they play in mitigating the risks and liability of these new devices. Who is responsible for any cybersecurity weaknesses? What is an appropriate contract or disclaimer notice that can be attached to such a device? What insurance is available to cover such risks? What are best practices for cybersecurity and product development to assure data privacy and security for consumers?

We are now also talking about how artificial intelligence or AI which allows systems to emulate human tasks without human intervention and that are connected with IoT devices. AI combined with IoT allows devices or systems to collect and exchange data without any human involvement.

One key issue to remain aware of is that it is often unclear whether IoT technology is a product, a service, or a mix of both. IoT technology could be subject to traditional product liability standards, so it is possible that either the software developer or the product manufacturer could be held liable in the event of damages caused by a malfunction. Assigning legal liability is particularly unclear if the IoT device utilizes Artificial Intelligence (AI). Currently, no laws address injuries caused by AI. Given how uncertain liability in relation to IoT devices is in the law, delineate liability as explicitly as possible in your contracts.

Many IoT devices use AI technology to function. AI is not a single technology, but rather a broad term for computer technology with the ability to simulate human intelligence. This simulated intelligence can take many forms: analyzing data and drawing conclusions about it, learning from data to perform tasks better over time, identifying patterns, predicting future outcomes, optimizing practices, and/or automating repetitive functions. AI can be very useful for businesses, which may use AI for anything from compliance monitoring to industrial robotics.

If you are acquiring a business that uses AI, carefully review the representations and warranties made by the vendor and ensure they adequately address the business impact of a system failure or malfunction. Additionally, you should be sure to scrutinize the non-infringement warranty. AI systems may produce infringing code when performing its functions without direction by the operator, and the issue of intellectual property infringement liability by AI systems is still unclear. Make sure the representations and warranties made by the vendor adequately allocate liability in the event that the AI system produces infringing code. You should also seek indemnification from a vendor to reduce liability in the event that an AI system's decision-making process results in a liability.

California became the first state to enact a law covering cybersecurity related to ‘smart devices” SB 327(2018). Effective January 1, 2020 any manufacturer of a device that connects “directly or indirectly” to the internet must equip the device with “reasonable” security features designed to prevent unauthorized access, modification, or information disclosure. If the device can be accessed outside a local area network with a password, it must come with a unique password for each device, or force users to set their own password the first time they connect. There can be no generic default credentials that might be discovered by a hacker.

The law covers any device makers who sell products in California. As a result this California law will likely be followed by most IoT device manufacturers as they will not want to give up the California market.

Oregon followed California’s lead and also passed a law to require manufacturers of internet “connected devices” that make, sell or offer to sell the devices in the state to equip the device with “reasonable security features”.

According to the Oregon law, “[R]easonable security features” means methods to protect a connected device – and any information the connected device stores – from unauthorized access, destruction, use, modification or disclosure that are appropriate for the nature and function of the connected device and for the type of information the connected device may collect, store or transmit.

Privacy and IoT

The volume and variety of personal data collected by IoT devices results in obvious privacy concerns. Fitness trackers and medical devices may collect data about a person's medical condition, location, and daily routines. Smart televisions can compile viewing history, preferences, habits, and other personal data. Cars may generate information on driving habits, movements, personal associations, locations, doctor visits, strip club visits etc. The pervasive monitoring of personal activities through IoT devices may not be what the individual expected or wanted. A person may not realize

that voice activation technology embedded in a smart device in their living room such as a smart television may be monitoring or recording private conversations. The use of IoT devices with artificial intelligence and mobile computing has increased the concerns regarding privacy and how such rights can be protected.

As discussed in the *A Legal Guide to Privacy and Data Security 2022* the United States does not have a single comprehensive federal law that regulates privacy and instead has a patchwork of federal and state laws based on sectors and industries along with some common law principles and limited constitutional authority.

IoT devices that utilize GPS for tracking may be closely scrutinized in any Fourth Amendment legal analysis. Did the individual know of the IoT product with the tracking technology? Did they have a choice? Was location of tracking private or public? Did the person have a reasonable expectation of privacy? The scope of this "reasonable expectation "of privacy legal theory will continue to be challenged in this new era of IoT devices.

As noted above the use of IoT devices span multiple industries including, medicine, health, transportation, and recreation. The FTC may be deemed the primary regulator of IoT devices due to it's broad mandate and authority to regulate consumer protection. Other agencies may get involved if the device falls within its purview such as the FDA for medical devices or the National Highway Traffic Safety Administration (NHTSA) for connected vehicles.

In any event the patchwork of federal, state, and global laws governing privacy and data security as covered in the *A Legal Guide to Privacy and Data Security 2022* will have to be considered where IoT devices are used to capture, store, or transmit personal information.

CONSIDER ISSUES OF CONFIDENTIALITY/DATA PRIVACY/ SECURITY

The legal landscape of data privacy and security law in our ever-changing technological landscape is unpredictable. It is important to stay up to date with federal and local legislation relative to data privacy and security law. Recent sweeping changes have taken place in Europe and California. In May 2018, the European Union General Data Protection Regulation (GDPR) became effective. The GDPR had a significant impact on how businesses collect, process, and store personal information. The California Consumer Privacy Act (CCPA) became effective January 1, 2020. Businesses that collect any data from California residents must educate themselves about the requirements of the CCPA and create a compliance plan. It is important to maintain a secure system with safeguards in place to limit your potential risk and exposure to any violations of data privacy rules and regulations. The most noteworthy aspect of the CCPA is the private right of action allowed in the event of a data breach. This statutory remedy will likely lead to many class action lawsuits. Agreements with vendors who process your data must be reviewed to make sure they fully comply with the CCPA and all other data privacy and security laws. It is equally important that your information and data is maintained as confidential, particularly personal information of individuals that is protected from disclosure as a matter of law.

The vendor agreement will likely include restrictions on use and disclosure related to vendor proprietary information. Review any restrictions on use of vendor information to make sure that the restrictions are not unreasonable and provide you with sufficient

flexibility. If your system is hosted, you need to make sure that these same safeguards are in place. It is essential to maintain confidentiality of data that is in the custody of a third party. These parties should employ firewalls and other appropriate security measures to make certain that there is no breach in security. Data privacy and security is of even more critical importance for regulated industries such as financial and healthcare organizations.

In the event of a data breach, you must comply with data breach notification laws. All 50 states, plus the District of Columbia and the United States territories, have statutes requiring notification of individuals when a data breach impacts their personally-identifiable information (PII). Typically, the jurisdiction in which the affected individual resides determines which law applies. Definitions of PII usually include social security numbers, driver's license and state ID numbers, and financial account information. Most statutes exclude data elements that are encrypted or otherwise unreadable and information that is legally publicly available from the definition of PII. Accordingly, one safeguard you should take is to encrypt PII that your business is processing and storing whenever feasible. For more information on data privacy and security related issues, consult the MN Department of Employment and Economic Development and Lathrop GPM joint publication *A Legal Guide to Privacy and Data Security.*[1]

[1] This guide can be found for free online at: https://mn.gov/deed/assets/a-legal-guide-to-privacy-and-data-security-2022_ACC_tcm1045-51497.pdf

BLOCKCHAIN TECHNOLOGY AND CRYPTOCURRENCY

Blockchain technology has become an increasingly popular way to solve a variety of recordkeeping and transactional issues. Blockchains are digital online ledgers that allow users to record transactions in a shared ledger and are implemented using a distributed ledger. Distributed ledgers are auditable, real-time digital lists of transactions and data that is distributed to network participants. Blockchain got its name because it gathers new transactions or other data into blocks, validates them using a consensus mechanism, and then connects or "chains" the validated block to the blockchain, which updates the distributed ledger.

A widespread use of blockchain technology is for cryptocurrency like Bitcoin. Cryptocurrency refers to digital interests that function as currency, but are not backed up by a regulatory agency, government, or centralized bank. To use Bitcoin, users need to have a set of "keys" that identify it for its Bitcoin transactions. These bitcoin keys are kept in digital "wallets," which are maintained by a number of service providers. These wallets are not always secure, and hackers have stolen Bitcoin keys and Bitcoins themselves by infiltrating these digital wallets. It seems unlikely that cryptocurrency will see widespread use in the near future for a variety of reasons, but blockchain technology is being ever-increasingly used as a recordkeeping tool.

Blockchain technology is also used in the creation and execution of smart contracts. A smart contract is a self-executing contract that obviates the need for third parties to a transaction. It does this by turning a contract into computer code that automatically executes the contract and transfers assets and then enforces obligations negotiated under the contract.

You may opt to use blockchain technology for its cybersecurity benefits. Blockchain applications provide strong security for networked ledgers, but are not invulnerable. Cyber-attacks often target centralized databases because they can infiltrate the entire system, and distributed ledger technology offers greater protection because an attack on one or a small number of participants does not result in system failure. Uncompromised members of a blockchain are able to maintain ledger integrity and availability and continue transactions. Additionally, blockchains transparency makes it less vulnerable to corruption via malware, because each participant holds an identical copy of the ledger, which makes it easy to detect modifications to the historical record. Blockchain technology may provide IoT devices to authenticate each other and ensure that their intercommunication is valid.

ASSURE SUFFICIENCY OF SCOPE OF USE

Does your license cover all of your intended uses?

In most cases the technology acquired for use in your business is made available through a license from the software vendor with restrictions on how and where the software can be used. Software is generally not "sold" but instead licensed. This "license" means that you are granted permission to use the software in your business but certain restrictions are imposed on your use of the software. While this is the common and standard practice for software it is important to make sure that these limitations are appropriate and do not overly restrict your intended use. Typical restrictions relate to the type of operating system or hardware permitted to be used with the software, or the number of computers, concurrent users, or facilities that can use the software. Many agreements will outline or define specific "permitted uses" or limit use of the software to the ordinary internal business of the customer. Vendors do not want you providing their software to third parties or possibly not even to a parent or affiliate, all of whom are potential additional customers and fee paying licensees.

Because of these restrictions in scope of permitted use, it is essential that you review the license grant and determine if the scope of use is sufficient for your purposes, both in terms of your company's strategic goals and its information technology operations and infrastructure.

- *Will the licensed technology be used by the entire enterprise or just a small group within the company?*
- *Will access be permitted through mobile devices?*
- *Is the number of users limited?*
- *How broadly may "permitted uses" be defined?*
- *Are you limited to only use the software on specified hardware or servers?*

You may also want to consider negotiating, in advance, any additional fees that may have to be paid in the future should the scope of your company's use change. For example, how much would it cost to add additional users or facilities? Other licensing and use considerations:

- *Is the license exclusive or non-exclusive?*
- *Does the license include the parent, subsidiaries or affiliates?*
- *How are affiliates defined?*
- *Do you get the source code that will allow you to maintain and modify the software or just object code?*
- *Distribution rights, if any, and extent?*
- *Rights to make modifications and derivative works yourself or with a third party?*
- *Right to allow system or software applications to be outsourced for operation by a third party?*
- *Rights to enhancements and updates as well as new releases?*
- *Does license accommodate your disaster recovery plan and ability to use third parties to host or maintain the software?*

COVER INTELLECTUAL PROPERTY RIGHTS, OWNERSHIP, AND PROTECTION

Software vendors have multiple customers that make use of the same software and the vendors will want to make sure that they can continue to market and distribute their products, including any derivative works, to as many customers as possible. For that reason the software is provided through a license and not a "sale." These customers may even include your competitors. While it is fair for the vendor to assert and maintain patent, copyright, and trade secret rights in software that they have already developed and made available for use in your business it might be appropriate to at least consider what intellectual property rights, if any, you might be entitled to as result of any customizations performed by the vendor. For example, if the project includes unique programming or significant modifications to the vendor software that is based on your specifications or special business requirements you might want to at least discuss ownership and the right to use of the new code.

At a minimum it should be made clear in the agreement with a software developer that any unique business processes or data that are used by the developer or included in the custom modification remain proprietary to the business owner and cannot be reused with other licensees. These discussions regarding newly developed intellectual property can lead to some interesting negotiations including the potential for royalties paid back to the business for any newly developed intellectual property. As the owner of the copyright in any preexisting software the vendor will have the exclusive right to make any derivative works.

Other ownership considerations include:

- *Will the vendor give the business owner the right to develop modifications to the software alone or through a third party and if so will the source code be made available for such purposes?*
- *Who will own the resulting derivative work?*

These are all questions and issues that should be considered whenever software development will be part of the system implementation.

New technology might provide you with a competitive advantage in the marketplace. If you are hiring computer programmers to develop new software or technology you might consider exploring patent, copyright, trademark, or trade secret protection in the technology. Each form of intellectual property has its own requirements and may or may not be appropriate for your transaction. It is important to recognize that unless considered a "work-made-for-hire" pursuant to the United States Copyright Act the copyright in any computer program remains with the person who wrote the code. It is essential therefore to cover ownership of any such rights in a written agreement. Without the written assignment, the computer programmer may retain the copyright in the underlying code.

ALLOCATE RISKS THROUGH INDEMNIFICATION

As noted above the buyer or licensee should obtain a warranty that the vendor has the unrestricted right to license the technology and that it does not infringe upon any third party intellectual property or property right. If a third party claim of infringement or misappropriation is brought against the licensee or user of the technology then the vendor should protect the user against any resulting loss or liability. These third party claims might seek monetary damages and injunctive relief preventing further use of the technology. The vendor might also be required to provide a means for the user to continue using the allegedly infringing technology or provide a suitable non-infringing alternative. This allocation of risk is fairly standard in technology agreements and would appear in the form of an indemnification and hold harmless provision. The vendor should assume this risk as necessary to insure that the user is relatively free from worry in the event of such claim by a third party.

ASSURE SUFFICIENCY OF USE OF THIRD PARTY SOFTWARE AND OPEN SOURCE

Make sure that the software vendor has the right to pass through any third party licenses, warranties, or rights especially those that are necessary to use any third party software that is linked to or embedded in the vendor software and is necessary for the software to operate. If payments are required for use of third party software make sure that vendor has paid the requisite license fees and that you are authorized and able to use the third party software.

Do you get support from the vendor or directly from the software manufacturer?

Of special concern is the growing use by software developers and vendors of what is known as Open Source (OS) software. This code is widely available and can be instantly downloaded at little or no cost. The OS code is still however covered by OS licenses that vary in what rights and restrictions are imposed on the software developer and user. You might seek a warranty from the vendor that there is no OS software included. If OS is involved it may be difficult to get warranties and indemnities from the vendor. The agreement should also warrant that no additional third party software other than what is specified or provided by vendor is required or necessary to operate the system.

UNDERSTAND THE IMPACT OF BANKRUPTCY ON SOURCE CODE

Source code is the form of computer code that allows a reasonably skilled programmer to modify and change the program. It allows for support of the program and the creation of enhancements or derivative works. It is also usually considered trade secret of the vendor and not readily shared with the customer. Instead of providing the customer computer source code, the vendor will usually provide a customer with computer software in object code machine readable format only. The customer is probably fine with not having source code so long as the customer will not be making any modifications to the code. The software agreement should however cover certain contingencies.

What if the vendor becomes insolvent or bankrupt and is unable to support the software?

Without the source code it will be impossible for the customer licensee to support the computer program or engage a third party to provide such support. Most vendors will cover such contingency by placing the source code in escrow with a third party and allow for release of the source code to customers upon certain triggering events. These events may include the filing of bankruptcy by the vendor or the inability of the vendor to support the program. The source code escrow agreement should be reviewed to assure that appropriate triggering events are included and that the source code is continually updated to conform to the most current software version in use. It is of no benefit to get a release of the source code from escrow and find that it is an outdated version that is not compatible with the version in your business operations.

The escrow agent should also be experienced in software escrow and allow for verification that the code on deposit is current and appropriate. Some software escrow agents will even (for a fee) perform such validation services to assure the beneficiaries that the code has been kept current. The payment of escrow fees should also be negotiated as part of the system software and license agreement.

NEGOTIATE REMEDIES

Watch out for any vendor attempt to assert a self-help remedy that allows, for example, the vendor to shut off the system without notice to the customer. This can be done through use of dongles, disabling codes or other technical means and can wreak havoc on a business.

The vendor can only legally pursue such a self-help remedy if it is clearly disclosed and agreed upon by both parties. In one well publicized case a software vendor disabled software used by the customer for inventory control after the customer had alleged problems with the system and withheld payments. As a result of the disabling code the customer was unable to process inventory or distribute its products. Millions of dollars were allegedly lost in missed orders and the defendant software vendor was found liable for damages. Customers and vendors should seriously consider whether or not the presence or use of disabling codes is appropriate and when, if ever, the activation of such codes is justified. As noted above it might be appropriate for the customer to include a warranty that there are no such disabling mechanisms in the software.

A business does not want to be surprised that their computer system has been shut down through the unilateral action of a vendor. Important remedy questions to consider:

- *What events give rise to a refund appropriate as a remedy for failed performance?*
- *Failed implementation dates? Failed support obligations? What about a refund as the sole and exclusive remedy?*
- *Are credits appropriate in the case of failure to meet service level requirements for support? What formula is used to determine credits?*
- *Are credits the sole and exclusive remedy for failed support?*
- *Is termination the sole and exclusive remedy?*
- *Can the customer obtain a replacement program or services and obtain reimbursement from vendor for the costs incurred?*
- *Liquidated damages or specific performance as an alternative remedy?*

Other delivery and completion considerations:

- *Is time of the essence in delivery and completion of the system?*
- *Is it appropriate to include a deduction or increase in fees in the event a performance milestone is reached or missed?*
- *Is it appropriate for the vendor to include early termination fees in the event customer cancels or terminates service?*
- *What transition services to a new provider are offered by vendor and at what cost?*

These considerations are especially important when hosting or related services are provided and the vendor has control of the customers' website and related content and information.

Finally, there are other repair and replacement considerations to factor in:

- *Are repair or replacement the sole and exclusive remedies?*
- *What if efforts by vendor to repair or replace are still not satisfactory?*
- *Are credits towards future maintenance appropriate?*

SPECIFY TERM AND TERMINATION

The ability for a vendor to terminate your software license may completely suspend your business or may impact how you transition to new available software. Some termination considerations:

- *What is the term of the agreement and the software license?*
- *Is the software provided under a perpetual irrevocable license?*
- *Is it provided under a subscription model with monthly or annual terms?*
- *What rights do the parties have to terminate the agreement and/or license?*
- *What obligations remain after termination?*
- *How and when will your data be returned or transferred to another provider?*

Make sure that the vendor cannot suspend service or use during any dispute. If system is outsourced or hosted make sure you cover the transition assistance necessary to move back to your site or to another provider.

DETERMINE LIMITATIONS OF LIABILITIES

Most agreements for technology will include a provision that limits the liability of the vendor.

It is common and reasonable for the vendor to disclaim any liability for incidental, special or consequential damages that are speculative and not foreseeable. The vendor should however remain liable for direct damages that are foreseeable, quantifiable, and the direct result of their actions.

There may also be a dollar cap imposed on any damages. In some cases the cap may be limited to the amount of fees actually paid by customer during the preceding 12 months or other limited time period. The cap could be extended to all fees paid regardless of when paid. It is reasonable for the customer to make an exception to any cap for damages that result from third party claims of infringement so that such claims and any resulting damages assessed against customer are not limited to the cap on damages.

The vendor might also try to reduce the statute of limitations so that the customer loses the right to bring an action against vendor if the lawsuit is not commenced in a timely fashion. These discussions and negotiations are all about allocating the risk between both parties in a fair and reasonable manner. The limitations of liability should be drafted in a way that the risk is reasonably allocated between both parties.

BE AWARE OF EXPORT CONTROL

Specific rules and regulations govern the use and distribution of software outside of the United States, with special attention given encrypted software and software designed for military use. These laws also apply to the use of the technology by persons who are not United States citizens. Penalties for violating these rules are substantial, so it is important to understand how these export control laws may restrict the ability of your business to make use of software, and to make sure that the vendor has obtained all clearances necessary to allow your business to make use of the software wherever it is necessary and by whomever it is necessary to use the software for the business. This is especially important if your business has a high level of foreign interaction, such as foreign travel or employment.

Standard license agreements often include provisions restricting a licensee from exporting the software in violation of any of export control laws, requiring licensees to obtain any necessary licenses or governmental approval prior to any export activities, and even mandating that licensees provide notice of the need to comply with these laws to any other entity using its licensed technology. Vendors should help make sure their customers are aware of what the export control restrictions if any are on the use of the software. You might also request that the vendor provide you with the specific export classification for the software that allows it to be used outside the United States. The vendor should warrant that the software as provided to the licensed customer fully complies with all export control regulations and provided assurance that customer can use the software as it deems necessary.

IDENTIFY JURISDICTION AND VENUE

The law governing an agreement, and the venues to which the parties to the agreement could be subject, are especially important in the context of technology licensing and system acquisition. As discussed above, there are many and varied federal and state laws governing the subjects of these contracts, and compliance can turn on the jurisdiction relevant to the agreement. Businesses operating across states or multi-nationally must comply with all applicable laws, especially those relating to data protection and privacy. Further, through Software As Service, online distribution of applications, and "cloud" computing agreements, jurisdictional hazards may arise based solely on where a business's data is stored, even if only temporarily.

Generally, a licensor chooses the law of the state in which it is based to govern such an agreement, as well as venue in the federal and state courts of that state. There is a reasonable basis for these choices since there is assumedly a strong relationship of the licensor to that state, including legal counsel that is familiar with its state's laws. However, licensees in different locations may also demand that venue is consented to in their state(s) as well. Due to internet hosting considerations, some agreements also specify the jurisdictions in which data may be stored or transferred, or in which services may be performed.

It would be advantageous for the licensee to have the vendor agree to jurisdiction and venue in licensee's home state. This may be difficult to negotiate with a vendor with a large number of customers as it could make for an administrative nightmare. If venue and jurisdiction become an area of disagreement a compromise may be to require the party initiating the litigation to bring the action in the other party's venue and under the laws of that jurisdiction. This provision also serves as a disincentive to litigation and may result in earlier dispute resolution.

CONSIDER TAXES

Scrutiny on the taxation of both software and internet-related transactions is continually evolving at both state and federal levels. Specific to the sale and licensing of software are the timing of revenue recognition and the classification of support services. Guidelines surrounding software revenue recognition in compliance with generally accepted accounting principles (GAAP) specify that revenue normally be recognized upon the delivery of the software. Some agreements, however, include acceptance testing provisions (discussed above) which allow the customer to test the software before accepting it for purchase. Because the GAAP guidelines require deferral of revenue recognition if there is significant uncertainty as to whether such revenue will be realized, it is important for agreements to be specific and definitive in any acceptance testing provisions. For example, criteria for acceptance or rejection should be listed, a narrow time frame should be provided for, and the vendor should require a formal sign-off by its customer of acceptance. Similarly, any rights of cancellation held by the customer prevent revenue from being recognized by the vendor. Warranties that contain anything more than short term and minor rights in this regard may be problematic for the vendor. The tax consequences for the vendor must however be balanced with the need for appropriate acceptance testing of the software.

The classification of support services also raises tax issues that vary from state to state. Computer software related services such as software support, maintenance, and custom software development may be exempt from sales and use taxes in certain instances. Some laws distinguish between maintenance and support in the form of direct services as compared to upgrades and enhancements. You will want to review the tax provisions specific to your state.

DETERMINE WHETHER TO LEASE OR PURCHASE

As most businesses have moved away from on-premises software and to the "cloud" the purchase of expensive computer servers and related hardware systems as decreased. A computer systems acquisition is still a major decision for any company, and the determination whether to lease or purchase outright laptops or an entire system, including hardware and software, is an important one. Certain business concerns might dictate which choice makes sense in a given situation, such as the business's available cash, necessity of staying updated with the latest technology, or the availability of technical support personnel. However, there are also legal and tax consequences associated with each option.

Parties to a lease agreement, for example, will want to clearly establish which, if any, updates or additions to the equipment by the lessee become the lessee's, rather than the lessor's property. Further, under a true operating lease agreement, a business's computer systems will be classified as a monthly operating expense rather than a depreciable asset. This gives the business the advantage of a steady and predictable monthly payment over time, and a relatively short lease time-frame (generally two to three years). Provisions typically included in this type of equipment lease include those relating to repossession, quiet enjoyment and payment of taxes, renewal, trade-in/upgrade rights, and any purchase options at the end of the lease.

With the outright purchase of equipment, on the other hand, a business can realize substantial tax deductions. Under Section 179 and Section 168(k) of the tax code (Section 168(k) is known as "bonus

depreciation"), businesses are allowed to deduct the full purchase price of certain qualifying equipment and/or software purchased or financed during the tax year in that first year of ownership. This is in contrast to an operating lease, which would only allow an expense deduction for each monthly payment. While Section 179 and bonus depreciation have existed for some time, theyhave become more of an incentive to businesses over the past few years. The limits for Section 179 and bonus depreciation deductions have increased, and changes to depreciation rules allow businesses to immediately write-off large percentages of the cost of depreciable property. Importantly, these deductions are available with certain types of leases as well – those that treat the equipment as an asset of the lessee. If a lease is treated as a capital lease rather than an operating lease for tax purposes -- which would often be the case if the lease includes some type of bargain buyout or purchase upon termination -- the leased equipment is treated as an asset of the lessee and can therefore qualify for Section 179 and bonus depreciation deductions. Some states do not conform to the federal Section 179 and bonus depreciation deductions, however, so you will want to review the tax provisions on depreciation specific to your state leases, most of which include some type of buyout or purchase upon termination provision, a business's equipment is treated as an asset and can therefore qualify for Section 179 deductions.

REVIEW INSURANCE

With any business, having the right insurance is a necessity. Many standardized vendor agreements attempt to allocate most of the risk to the customer. Because of this, businesses should check their insurance policies to determine whether business interruption insurance covers vendor failures. Some equipment lease agreements may also require the lessee to insure the leased equipment, so a business would want to ensure their property coverage was sufficient. From a vendor's perspective, professional liability insurance can protect against professional negligence that causes loss of client data or software or system failure. Large and small hardware and software producers and servicers are all at risk for professional liability suits, and would benefit from this type of insurance. You might also require that the vendor carry insurance in appropriate amounts with you as a named insured.

Cybersecurity insurance has come a popular mechanism for managing risks and costs related to data breaches. Coverage for legal advice, computer forensics, fines, and notification costs are usually covered in such plans.

The private right of action in the California Consumer Privacy Act allows statutory damages to be recovered in the event of a data breach and a business has failed to maintain reasonable data security.

Now may be a good time for a business to have cybersecurity insurance that covers such potential legal claims.

COMPLY WITH THE UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT

The Uniform Computer Information Transactions Act (UCITA) is a uniform law that is only enforced in those states that have adopted it. Since proposed in 1999 it has only been adopted in Virginia and Maryland. It attempts to govern software licenses and includes sections related to the enforceability of shrinkwrap and click on licenses as well as providing rules for what law governs, how to treat online agreements, and what default rules apply in the absence of anything in the software agreement. The Act has not been without controversy and is generally perceived as a pro vendor law. You may see language in some software agreements that requires the parties to opt out of coverage. Depending on your transaction it might be wise to opt out of UCITA coverage and check to see if it applies to the jurisdiction of your agreement.

NEGOTIATE MAINTENANCE AND SUPPORT

When does the maintenance and support service begin?

Maintenance and support of the system should be negotiated and included as part of any agreement. Maintenance and support fees are significant sources of revenue for vendors. In some cases an initial license fee may look low but annual maintenance and support fees become exorbitant. When considering the total costs to acquire a system it is important to look beyond the initial purchase and license fees. Consider not only the initial maintenance and support fees but what these maintenance and support fees will look like over the next five years. Vendors are usually willing to provide some cap on future increases in the form of an annual percentage or tied to the Consumer Price Index. You might be able to negotiate no increases for a limited number of years.

If a performance warranty for a limited period of time is offered (such as 90 days or one year) you may be able to negotiate free maintenance and support during the limited warranty period.

The potential for obtaining maintenance and support form a third party, particularly in the case where the vendor becomes insolvent or is otherwise unable to provide necessary support should also be covered in the agreement.

- *Exactly what is included under maintenance and support?*
- *Are both hardware and software covered?*
- *Do you have one vendor you can look to for system maintenance and support or do you have to seek support from multiple vendors?*
- *What happens when one vendor points the finger at another?*
- *Are software upgrades and enhancements included under maintenance at no additional fee?*
- *How are new products sold by the vendor that require additional license fees distinguished from upgrades covered under annual maintenance fees?*
- *What is the process for giving notice of any malfunctions or deviations from the expected performance of the system?*
- *How soon will the vendor respond to any issues and correct the problem?*
- *What remedies are available for failed support?*
- *What service levels, response times, and availability are provided?*

CONSIDER UNIQUE ISSUES FOR FRANCHISED OR FRAGMENTED BUSINESS SYSTEMS

Although the considerations in this guide are equally applicable to large organizations and small start-ups, there may be special considerations for franchised or licensing-based systems when reviewing technology agreements. Franchisors or licensors must carefully consider whether their franchisees will enter into direct agreements with any vendor or sign an end-user agreement with the franchisor—each of which come with their own cautionary tales. With the increasingly complex framework for state privacy and data-protection, franchise systems that collect personal data may want their franchisees to sign directly with the vendor, while other franchisors may decide data access is more important and want the franchisees to sub-license for the use of technology.

Franchisors should carefully review any agreement between a technology vendor and franchisees to ensure that termination of the franchise agreement serves as grounds for immediate termination of the technology license agreement. If a franchisee is sub-licensing for technology through the franchisor, the franchisor will want flexibility to expand the system or change technology requirements, but be careful to not take on liability for data breaches or for technology failures on the part of the vendor.

COMPLY WITH LAWS AND REGULATIONS - SPECIAL CONSIDERATIONS FOR HEALTHCARE RELATED BUSINESSES

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH) and related privacy laws, rules and regulations have had a profound impact on the collection, storage, and use of healthcare related information by healthcare related organizations and businesses that service them. You may be covered by HIPAA or HITECH as a so-called “covered entity” or as a “business associate”

In some respects, health-related technology using cloud service providers has outpaced relevant HHS guidance on how to use cloud service providers without running afoul of HIPAA. In 2016, HHS clarified that most cloud services used by HIPAA covered entities would be considered business associates. This business associate status applies even if the cloud service merely encrypts personal health information, rather than stores it.

Practically speaking, if your business is a covered entity, or a business associate of a covered entity, that is going to engage a cloud service provider, there are three best practices you should be mindful of. First, it is important to conduct an independent risk analysis of the cloud service provider’s for vulnerability to personal health information. Second, establish risk management policies. Third, enter into appropriate Business Associate agreements.

Achieving and maintaining compliance with HIPAA and HITECH requires significant organizational effort. Data privacy rules and regulations continue to evolve and must be monitored for any changes. If you are required to comply with HIPAA or HITECH it is important to select a vendor and a solution that are able to make the requisite changes to the system in a timely, efficient, and cost effective manner, and to require such actions as part of the agreement. You should also be prepared for a data breach and have a plan in place along with your vendor to deal with such an event.

New practices and procedures may have to be implemented to assure compliance, security, and the maintenance of privacy and security of patient identifiable information. Compliance with these data privacy and security laws is not just an issue to be resolved simply through the acquisition and use of new information technology. Data privacy and security is a challenge and opportunity for the entire organization to embrace through training and education that is implemented in conjunction with efficient, effective, and secure information technology.

RECOGNIZE THE TYPES TECHNOLOGY RELATED AGREEMENTS

The following is a list of the types of agreements that you might encounter:

Software license

System (hardware and software) agreement

Click-on, shrinkwrap, browsewrap licenses

Open Source licenses

Services and consulting agreements

Maintenance and support agreements

Software development agreements

Outsourcing agreements

Website development and hosting agreements

Application Service Provider (ASP) agreements

SAAS (Software as-a- service) agreements

Platform-as-a-service (PaaS)

Cloud related agreements

Disaster Recovery agreements

Data Processing agreements (DPA)

Asset Purchase agreements

Alpha/Beta Test agreements

HIPAA Business Associate Agreements

Software Distribution/Reseller agreements

VAR/OEM agreements

Employment agreements

Confidentiality and non-disclosure agreements

Patent, copyright, trademark, know-how and hybrid intellectual property licenses

Smart Contracts

DON'T TREAT THE CONTRACT AS AN AFTER THOUGHT

Your information technology is a vital corporate asset capable of providing a significant competitive advantage in the marketplace. More and more it is also becoming critical to your compliance with certain federal, state and even global laws and regulations. Agreements covering such technology should be treated with the highest level of care and concern. The same level of scrutiny should be given these agreements as any other business agreement involving a significant corporate asset.

A clearly written reasonable agreement may not guarantee success or prevent potential risk and liability but it can serve as an active tool to ensure a smooth and efficient implementation. It can also provide an opportunity to consider foreseeable events and their consequences. The agreement itself should be considered as more than an enforcement tool in the event of litigation. Make use of the agreement early in the acquisition process as an opportunity to educate both parties on the business venture and to create a relationship based on trust. The agreement can also serve as a means to manage the business relationship, encourage communication, and reward achievement.

The process of acquiring a computer system or transitioning to a new technology platform should not be an intimidating one. With proper planning, it should result in a more efficiently run and successful business. The contract should not however be treated as an afterthought. The agreement should be fair in its allocation of risks and liabilities and represent an accurate reflection of both parties' expectations and responsibilities.