Negotiating and Drafting Municipal IT Contracts

BY: LARA MAINELLA, *Assistant City Attorney, Madison, Wisconsin;*
PATRICK BRYANT, *Associate General Counsel, New York City Department of Information Technology & Telecommunications;*
CHRIS MALCARNEY, *Divisional Deputy Solicitor, City of Philadelphia;* PHIL LAM, *Deputy City Attorney, City of Los Angeles; and* EUGENE HSUE, *Assistant City Attorney, City of Philadelphia.*



INTRODUCTION

Negotiating a technology contract with a vendor can be challenging, due to the leverage some large companies may enjoy and the ever-changing nature of technology itself. In this article, practitioners from large to mid-size cities attempt to guide fellow municipal attorneys through perennial concerns, and share tips and tricks which we ourselves have found useful.

I. Types of Technology Contracts and Corresponding Concerns – Lara Mainella, Assistant City Attorney, Madison, Wisconsin

Cities require a variety of technology solutions to maintain operations and provide services to the public. This includes everything from software to run the payroll system, manage police reports, maintain public transit schedules, and provide vehicle diagnostics and telematics, to appointment scheduling and text message notifications for the public, to name just a few. It is important to recognize "what" your client is purchasing when evaluating and negotiating the contract – both the format of the technology, and the subject matter and data that the technology will manage.

The *format* of the technology determines the nature of the contract. This section will address the following formats: On-premise software, cloud computing services, and hardware.

Software: On-premise software is installed or downloaded to a local device such as your computer (the old floppy disc) or a server on the City's network. On-premise software is licensed, not sold, and your client will be presented with a click-through license agreement or EULA (end-user license agreement) that must be clicked and accepted to download or install, or a written license agreement for signature. Concerns with click-through agreements include: Does the employee installing this software have authority to bind the city to a contract? Can you negotiate the terms? Does the EULA contain legal terms that your city cannot, or should not, agree to? Do you want to negotiate every $500 software purchase? What are the risks?

"On-premise" is no longer the most common way to buy software, but it can be the most straightforward to negotiate, if the vendor is willing. If not, the above considerations might be business decisions for your client. Depending on a project's size or importance, you might advise them to select another vendor who *will* negotiate. Your client may decide the cost-benefit analysis does not favor spending legal resources on small software purchases.

When presented with a traditional on-premise software license, review it like any other contract – look out for binding arbitration, choice of law, shifts of liability. Some common but unfavorable clauses include dollar caps on the vendor's liability, city indemnification of the vendor, lack of indemnification by the vendor, one-sided termination provisions, and/or shortened statutes of limitation. Many software licenses include a concession that the vendor will suffer irreparable harm if the license is breached or their intellectual property is infringed, and the vendor is entitled to injunctive relief without having to prove it, and without posting a bond. Consider striking such concessions and changing them to say the vendor may "seek" injunctive relief. Finally, consider how to add any man-

datory legal terms required by your city, such as insurance, indemnification, social responsibility clauses such as nondiscrimination, and so on.

The next category is cloud computing, including **Software as a Service (SaaS)**, **Platform as a Service (PaaS)**, and **Infrastructure as a Service (IaaS)**. Cloud computing is provided via a public, private, or a hybrid cloud. "Public" refers to a third party that offers cloud services over the public internet to everyone – such as Amazon Web Services (AWS) and Microsoft Azure. Data can be segregated within tenant spaces and geographic limitations are possible, but not automatic, and probably not cheap. A private cloud is one that is used by a single company. PaaS and IaaS are delivered in a private cloud. **SaaS** is a software application hosted in a public, private or hybrid cloud and accessed by the user via the internet. Because these are such technical concepts, unless you're an expert, any cloud computing solution should be vetted by IT professionals long before the decision to purchase and contract, is made.

SaaS is software that would have been installed on-premises in "the old days" and SaaS subscriptions are the modern replacement of the on-premise license. A SaaS subscription provides software access, regular updates and maintenance, and technical support. Maintenance and updates are performed without your involvement and without having to touch your network - eliminating the extra fees and contract documents that come with annual maintenance of on-premise software. The subscription may also include training and other professional services. If the SaaS application generates or handles data, which most do, this data is stored (hosted) by the vendor or a third-party data center (aka public cloud). SaaS can be a low-cost way to provide functionality and save storage space. But the off-site storage of city data presents legal concerns: public records requests and retention, data ownership, data mining, security and back-up - discussed in Sections IV and V, below. Ideally, your IT staff will analyze security and back-up risks before deciding to buy SaaS; then, the SaaS agreement should address these things.

SaaS agreements are structured as service contracts, granting access to the service for a subscription period, in exchange for a fee. SaaS might be sold per user, or for an unlimited number of logins. It may or may not include a license grant, but there are restrictions on acceptable use and clauses protecting the vendor's intellectual property. The unfavorable clauses in most on-premise licenses are also present with SaaS. The customer must warrant that it will not upload harmful or malicious material, allow unauthorized access or sharing of

Continued on page 14



Lara M. Mainella is an Assistant City Attorney for the City of Madison and a graduate of the University of Wisconsin Law School. She has been negotiating contracts for the City for nearly 20 years, focusing on software and technology procurements. Lara assists the City's Purchasing and IT Departments on everything from click-through EULAs and "free trials" of software, to complex system implementations and transitions from on-premise to hosted solutions. Her hobbies include trying to convince social media platforms to agree to the City's mandatory terms and conditions. Lara can be reached at LMainella@cityofmadison.com.



Patrick Bryant is Associate General Counsel at the New York City Department of Information Technology & Telecommunications and focuses on IT procurements including public safety and cyber security. He negotiated the City's largest reseller agreements, drafted its first Resiliency attachment to a franchise agreement and assisted in negotiating the first-of-its-kind LinkNYC franchise agreement, providing gigabit-speed free public Wi-Fi and phone calls. He was previously Mayor Bloomberg's Deputy Chief of Staff for Legal Affairs. Patrick is a graduate of New York University School of Law, and has an MBA and Master's degree in accounting. He can be reached at pbryant@doitt.nyc.gov.



Chris Malcarney is a Divisional Deputy City Solicitor for the Intellectual Property Division of the City of Philadelphia Law Department. He drafts documents and leads negotiations for a wide variety of complex technology transactions, including SaaS, hosted solutions, ASP agreements, software development, licensing and escrow agreements, and maintenance and support agreements. Chris also negotiates consulting and professional services agreements, managed IT services contracts, RFPs and hardware procurements, as well as data licenses and business associate agreements. He is a graduate of Elisabeth Haub School of Law at Pace University and reachable at Christopher.Malcarney@phila.gov.



Phil Lam serves as the first Intellectual Property Counsel for the City of Los Angeles, and founded the first governmental intellectual property law practice in North America, developing the City's IP Asset Management program and IP licensing practice. He provides counseling, transaction and litigation services related to patent, copyright, trademark, entertainment, computer, privacy, and Internet laws, as well as major-asset acquisitions. He graduated with honors from Loyola Law School, Los Angeles and holds a Masters in Engineering from the University of Illinois. Before becoming an attorney, he was an engineering manager in the energy and aviation industries. Phil can be reached at phil.lam@lacity.org.



Eugene Hsue is an Assistant City Solicitor for the Intellectual Property Division of the City of Philadelphia Law Department. He negotiates cloud services, hardware, and software contracts, and counsels on proprietary rights and data security and confidentiality. Before joining the IP Division, he litigated in the Law Department's Right to Know Division, winning 18 appeals exempting public records from disclosure. He previously served as the Head of Research at the Second Circuit Library, is fluent in French and Mandarin and holds a BA from Cornell University, a JD from Temple University Beasley School of Law, and a MLIS from the University of Pittsburgh. He can be reached at eugene.hsue@phila.gov

passwords, or enable similar acts.

As with on-premise software, the vendor should offer to indemnify and defend the customer from third-party infringement claims. These are reasonable things. Less reasonable are clauses where the customer warrants that content uploaded to the system complies with all possible privacy laws, everywhere. Also unreasonable is requiring the customer to indemnify and hold harmless the vendor, their affiliates, and unknown third parties against all sorts of claims. While vendors will insist they need this to stay in business, most vendors will remove such an indemnity clause. You may have a harder time removing or raising liability caps (see Section III). The most time-consuming negotiation topic after limitations of liability is data ownership. Assume that your client has a quote for SaaS that will provide amazing efficiencies for city operations for only $395/month. In exchange, the vendor gets unrestricted access to your city's valuable data, allowing the vendor to use your data for whatever they want, even sell it, as long as it is de-identified and/or in aggregate form. There are two common clauses: one that allows the vendor to crunch your data solely to provide services to you, and improve service delivery. But a second clause might grant them ownership or a very broad license to use your data for just about anything. Try to learn the nature of the data - should it be analyzed, owned, or sold by this vendor? How sensitive is the data? How valuable is it? Can you strike that clause? (See Sections IV and V.) Educate your client about these risks. Finally, after removing unfavorable language, add the clauses your city requires.

Privacy Policies and Online Terms of Use (TOU): A thorough SaaS agreement may incorporate the vendor's Privacy Policy and Terms of Use for their website. How much attention should you pay to these? It depends, again, on the nature of the data. Often the privacy policy only impacts personal information of the employee who sets up the account. Or, privacy may overlap with the Confidentiality clause – read both. Online TOU might only apply when visiting the website. Ideally your negotiated SaaS agreement should integrate with or *supersede* conflicting privacy policies or TOU on the website or while logging in. After all that hard work negotiating your SaaS agreement, you don't want employees clicking on the TOU and setting up a conflict.

Service Level Agreements (SLA): This is a set of minimum requirements for "uptime" for the service - reflected in "nines" such as 99.99% availability. The SLA is often non-negotiable-but you should be aware of it. An SLA should not include legal terms but might limit your client's remedies for downtime or other performance lapses, such as deadlines for reporting downtime and being compensated for it. The client should review and approve any SLA.

What kind of Software?: A special situation arises when the vendor *doesn't know* if their product is on-premise or SaaS. You're pretty sure your client is buying SaaS, but the vendor gives you an on-premise license. Send it back and ask "are you sure this is the right agreement for this product?"

No Software: Maybe there is no software involved? Online training or other web-based content may not involve a license for any software-one less document to review! This raises the question of how involved you want to be in these purchases (or how much money the client wants to spend). Have a mutual understanding with your client, train them to spot issues and bring agreements to you sooner than later.

Hardware: Staff should be able to purchase *equipment* without legal help, right? But what about equipment that comes with software? Surprise–your client must sign a license agreement that comes with a printer / card reader / fingerprint machine / and so on. This is sometimes called "firmware." Firmware may not prevent security risks or data concerns, but you still must agree to a license agreement or the hardware won't work. Treat this like an on-premise license agreement.

Some equipment comes with "back-office" software (on-premise or SaaS) to operate the equipment or read data generated by it. (Parking access and surveillance systems come to mind). The agreement for the software that operates these systems should be negotiated like any other software agreement, and staff should be trained to ask for these agreements *before* buying equipment.

This is just a taste of some technology contracts and the legal issues presented. Even the most technologically challenged municipal attorney can become familiar with technology contracts, and develop your own strategy for negotiating them.

II. Statement of Work and Agile Procurement Process – Concerns and Risks – Patrick Bryant, Associate General Counsel, New York City Department of Information Technology & Telecommunications

Statement of Work vs. Scope of Work: Many technology contracts will require professional services to implement the solution. The acronym SOW is often used for Statement of Work and Scope of Work, often interchangeably, for the document that describes the work to be performed. For my purposes, I will be talking about the "statement" as the SOW. The *statement* of work is the larger document with more information than the *scope*. For most of our agreements, the

SOW will be an attachment to the agreement (the body of the contract that includes the boilerplate). The scope of work is a portion within the SOW. In addition to describing what the work actually is, the SOW could include a timeline, performance criteria, schedule of deliverables, travel requirements, location, special skills, and so on..

If the agreement is the brains of the contract, spelling out the legal arrangements between the parties, the SOW is the heart of the agreement. It's where the rubber meets the road. The SOW should be drafted jointly by the vendor performing the work and your city's business team who know their business needs, what the solution does technically and what proper performance looks like. They can evaluate deliverables. Business teams are often in a rush to buy something and may want to worry about the details later. I have reviewed SOWs, and I've literally seen some that are comprised of only five to ten bullet points with general descriptions of deliverables, and sometimes no real acceptance criteria. This is unacceptable. The SOW needs to be very, very specific. This is important both up front and on the back end. This is where you spell out exactly what you are buying, and exactly how you know if you got what you paid for when you were supposed to get it.

You may find yourself in the situation where you have to ask very basic questions of your business teams to help them draft a document that protects them. The most common question I find myself asking is "where does it say that?" For example, the draft SOW might say "Vendor will provide licenses so users can perform tasks." And I'll ask how many licenses? Which tasks? The business team then might tell me they are supposed to get 1,000 licenses where all users can perform task X, Y, and Z. And I'll ask where does it say that? If the vendor provided 500 license that allowed users to perform tasks X and Y, then the vendor may have a claim that it has performed under this ambiguous language. At this point your business team may be shorthanded; at best they have a dispute on their hands, and at worst they have wasted money for a partial solution.

You want to also focus on any assumptions the vendor writes into the SOW. For example, you can go to your team and say, "here is a list of ten things the vendor is saying are not in the scope; do you agree?"

Acceptance Procedures: Your SOW should provide clear procedures for when and how you will receive, evaluate, and accept deliverables. You have may have procedures that apply to all deliverables, documents deliverables, and/or releases and systems. Those will be project-specific. In a Systems Integration procurement for example, we have Preliminary Acceptance: this is when we agree that the system is ready to go into a production environment. Preliminary Acceptance is followed by Final Acceptance, which occurs when the system performs for 30 consecutive days in the production environment with no Severity Level 1 or Severity Level 2 errors (or an accumulation of enough Severity Level 3 errors to be deemed Level 2). Acceptance procedures will, of course, be project-specific.

A type of acceptance you should never have, however, is "deemed acceptance." This is when the vendor wants the mere passage of a certain amount of time to constitute acceptance. All of us who work for municipalities understand that in normal times, and especially given recent times, budgets and staff are thin. Deliverables should only ever be accepted if someone has time to review and accept them by checking against specified criteria. Two weeks going by does not mean the vendor submitted an approved deliverable. This is also something to look out for in the assumptions. Vendors tend to write language around review and acceptance of deliverables, but there is always the possibility that deliverables will need to be rejected.

What happens if a deliverable is rejected? This is important to note as vendors often draft SOWs with language similar to "Customer will have X business days to review and accept a deliverable." I always insert "Customer will have X business days to review and accept ***or reject*** a deliverable." The deliverable may be horrible. If there is a dispute on the back end regarding performance, the SOW is where you look. The remedies will be in the Agreement, but if properly written, then the answer should be in the SOW.

Use of Resellers: When we use a reseller, and we do it often, we have the reseller execute the SOW on the reseller's letterhead. This effectively creates a relationship in which the reseller is the prime contractor and the OEM is the subcontractor. The reseller is then responsible directly for delivering the services regardless of the entity who is actually performing the services. This makes sense because the reseller is the entity to whom we make payments.

It is often the case that software or cloud is part of the purchase, and if so, we separately execute the corresponding EULA or cloud services agreement directly with the OEM in order to have privity of contract with the OEM for the licensing terms. In this situation, we often have a pre-negotiated SOW template in place with the reseller. Obviously most purchases will differ on the details, so there should be some flexibility baked into the template. The flexibility should be specifically for things like business, technical and operational terms, but not legal terms. The SOW should not include things like indemnification,

Continued on page 20

limitations of liability, or termination rights. These terms are in the primary agreement with the reseller who serves as the primary contractor. Some basics in the SOW may be: points of contact for the project, payment terms (depending on how the main agreement is structured) with milestones, the scope of work baseline, change order process, acceptance, service levels, and miscellaneous non-legal terms.

In a direct-seller arrangement, the concepts are largely the same but at the very least (1) there is a layer removed, (2) the procurement method will be different, and will likely vary based on the dollar amount of the purchase, and (3) the procurement will take much longer in most cases. These concepts also carry over whether or not your development is a traditional "waterfall" development or an "agile" development.

"Agile" versus "Waterfall" Development: Some municipalities will have large units of inhouse developers, and some will exclusively rely on vendors to develop their software. The main concepts of agile development remain the same either way. Agile development is a response to traditional waterfall development. In traditional waterfall development, the entire process is essentially finished before the bulk of testing happens. Agile takes an incremental approach to processes that don't progress in a sequential, stepwise manner. Teams work across silos in a collaborative approach. The point is to have much shorter and more frequent feedback loops with the goal of addressing and fixing issues along the way. Agile works through a framework called "Scrums" which is comprised of "Sprints." For the purposes of an SOW, the concepts you want to focus on are pretty much the same, but the milestones and deliverables will typically need to be written in on a more frequent timelines, and the cross-functional teams, along with the developers will need to be more collaborative.

III. Limitation of Liability and Indemnification – Chris Malcarney, Divisional Deputy Solicitor, City of Philadelphia Law Department

Limitation of liability: Limiting liability is among the most important concepts in a commercial contract because it goes a long way in allowing both parties to gauge the extent of their risk when entering into an agreement. That said, since a customer's main duty in these types of agreements is often limited to its payment obligation, government contractors for goods and services may be able to avoid limitation of liability clauses completely. Vendors can be persuaded to forego a limitation of liability because of the predictable nature of the attendant risks in those types of contracts. For instance, if the contract is for a hundred desks, it's fairly easy to foresee the types of damages that could accrue from that contract. Additionally, when dealing with fungible goods such as desks, the customer has significant leverage because they can presumably procure such goods from another source without too much effort.

However, technology contracts are a different animal altogether. Damages are not necessarily proportionate to the dollar value of the contract. Even a small dollar contract or some freeware can contain viruses or bugs that allow data to leak out or hackers to gain access to a system. Stories of ransomware attacks routinely appear in the news, and one has only to scan their own personal email accounts to see notifications of data breaches. By the industry's very nature, it would be an unsustainable business model if technology companies had to pay for all of the damages that they caused. Technology contracting is also unique in that products and services are seldom considered fungible by the end user. Take mobile phones as an example: Androids, iPhones, Google Pixel phones, and others , are all capable of performing similar functions, yet many people, myself included, have strong opinions about which is the superior product. When clients become convinced that one technology solution is superior to other similar options, it can undermine the lawyer's leverage during negotiations. This tension between protecting your organization and participating in an industry that has increasingly grown both risk-averse and aware of its increasing leverage is one of the biggest challenges in negotiating technology contracts.

Obviously, the higher the limitation of liability the better for the buyer, whose real obligations are likely to be mostly the aforementioned obligation to pay the contract price, but whose risk is disproportionately higher due to the usual issues which may crop up during implementation or go-live, as well as the increasing specter of security issues such as data breaches and ransomware attacks. A formula that works well is to have the limit be the greater of a certain threshold amount or a multiplier of the total contract amount. The benefit under this method is that a multiplier of the contract amount will allow the level of damages to be proportionate to a contract that is amended beyond the initial value, while having a threshold amount guarantees that even if it is a small dollar contract, the aggrieved buyer can regain some of their losses.

Even when agreeing to limitation of liability, certain causes of action should be exempted. These include injury or death (likely excluded by public policy anyway but best to cite them out of an abundance of caution), property damage, and infringement of third-party's proprietary rights. It should be noted that this last category of proprietary rights in-

fringement has long been an industry standard carveout from the limitation of liability cap. There are vendors who will try to nibble away at the margins to reduce the risk, but as discussed below, this is a responsibility that should fall squarely on the shoulders of the vendor. Finally, if applicable, you should reserve the rights available under any sort of tort claims act that is relevant to your organization.

Indemnification: While breach of contract and/or warranty will provide a cause of action for aggrieved buyers, it is helpful to have an indemnification clause in the contract as well, so that a vendor will have to "step into the shoes" of your organization in the event that there is an action for which they are responsible. For government entities, these indemnity clauses are often one-sided as it is not considered good public policy to use taxpayer funds to indemnify vendors. Obviously, the broader the clause the better from the perspective of the government buyer, but it is frequently a challenge to get vendors to agree to an open-ended indemnity, so for most damages, an indemnity based on negligence is a reasonable fallback. Once again, however, indemnification for infringement of a third party's proprietary rights is distinct from the general indemnity case and should therefore be set forth in its own section or otherwise distinguished for the sake of clarity.

While there is often significant pushback about a general indemnity, the technology industry as a whole still generally recognizes that it is the vendor's responsibility to provide an indemnity for infringement of a third-party proprietary rights. This is likely because the customer has no way of determining what was used to create that software solution. Only the vendor can properly vet the components that make up the solution. So, for instance, if a vendor decides that it is financially advantageous for them to use open-source software as a building block when developing their solution, that is their prerogative, but they should not be allowed to pass the risk on to the customer of not having properly secured the rights to use that building block. Remember, one of the things that the customer is paying for is the peace of mind that the vendor has secured all necessary rights to sell what they are purporting to have the rights to sell.

These clauses usually require the vendor to provide comprehensive indemnification for infringement claims, but there are often several key qualifications. One is that the vendor has the rights to control the litigation and/or settlement of the matter. Two, the customer needs to provide reasonable assistance in the defense of the claim. And three, there is usually a series of solutions that the vendor may pursue prior to the contract being terminated in the event of the vendor not being able to secure the rights. Most frequently, the vendor will have the ability to attempt to cure the infringement at its own expense by: procuring the rights for the customer to continue to use the software; replacing the software with non-infringing equivalent; modifying the software to make it non-infringing; or in the event that there is no other option, requiring the customer to remove the software and refunding any amounts paid back to the customer. This last point can be contentious, with vendors taking the position that the customer will be unjustly enriched if it has been able to use a system for a time and then have receive a complete refund. The counter argument is that the vendor is being unjustly enriched because it benefited from the sale of a license to which it did not own the rights.

Several contingencies can let a provider off the hook for infringement. For instance, if the customer failed to install updates or enhancements for the software, if the customer modified the software or used it in a manner not intended by the parties, or if the software somehow became infringing when combined with unauthorized third-party software, then the vendor may have a credible justification to be relieved of its indemnification obligations because the customer neglected to take obvious steps that would have mitigated the infringement.

There is no one size fits all solution when it comes to limitation of liability and indemnity issues in technology contracts. A number of factors can impact negotiations, such as if the solution is "sole source," or if the client has very strong feelings about one solution being far superior to the others on the market. In all instances, it's best to consider the entire risk profile of a given deal (sensitivity of the data, complexity of the project, past relationship with a longstanding vendor, etc.) when advising the client if the terms are acceptable.

IV. Cyberliability Insurance, Cybersecurity Standards and Audits – Phil Lam, Assistant City Attorney, City of Los Angeles

Ransomware: Cyber-ransom[1] is a serious topic for both the private and public sectors, which the federal government supports with excellent resources[2] along with private information-sharing organizations.[3] Although this article is not focused on that thorny problem, effective cybersecurity provisions in vendor contracts could lower such business-freezing risks in addition to curbing clients' liabilities from garden variety cybersecurity breaches.

Cybersecurity is fundamentally an IT client's responsibility.

Cybersecurity contractual provisions: That said, comprehensive contractual provisions could reduce the chance of cybersecurity breach by making explicit a client's chosen standards,

Continued on page 35

IT Contracts *cont'd from page 21*

vendor's compliance responsibilities and their liabilities in the contract. However, there are no "standard" or one-size-for-all cybersecurity provisions, because the IT service business models, technology, cybersecurity standards and hackers' *modus operandi*, among other parameters, are constantly and rapidly changing by the months.

May I recommend the following major steps at the outset of any transactions involving data of any kind: (1) involve the most knowledgeable clients (MKCs) in cybersecurity and in the business needs of that particular transaction; (2) identify the data involved; (3) determine the desired cybersecurity standards to impose; (4) apply state, federal and foreign data privacy laws; (5) draft cybersecurity and data privacy provisions with priority consideration against other provisions of the agreement; and (6) add any applicable non-data privacy laws, if desired, to restrict unauthorized disclosure, use and sharing of data.

Involve the MKCs.: Involve in the working group, the client(s) most knowledgeable on current cybersecurity practice and standards (typically the Chief Privacy Office, Chief Data Office or Chief Cybersecurity Office) and the client(s) most knowledgeable about the business needs to be fulfilled by the transaction.

Identify the Data and Use: Through in-depth discussions with clients, identify the data (pre-existing and newly collected or created) involved in the transaction, and ask who may access, how and when. Nature of the data triggers different data privacy laws--state, U.S., and foreign. For examples, Protected Health Information,[4] Personally Identifiable Information[5] and Payment Card data are among the most sensitive and more regulated than anonymized inventory data. In addition, it is highly recommended that clients go through a checklist of data rights as in the "who, how and when?" questions for vendor and any third parties, including sublicensing right. Such data rights should be clearly included in the vendor contract. In separate provisions, typical intellectual property rights, including that in data, should be delineated in terms of who owns what IP and who holds a license (or even sublicense) and the scope of the license(s).

Desired Cybersecurity Standard(s): The MKCs should be dictating the technical and cybersecurity standards for the transaction based on their particular business needs and prevailing cybersecurity standards. The most popular international and U.S. cybersecurity standards, as of June, 2021, include ISO 27001 and SOC 2.[6] Though both are similar, SOC 2 requires auditing only by a licensed CPA. Because of the rapidly changing IT environment and threats, it is prudent not to stipulate in the agreement to a particular standard exclusively. A non-exclusive drafting could be useful, if a standard is to be specified by name. Alternatively, the agreement could use general term in describing "prevailing," "leading," or "industry cybersecurity standards" or words to that effect, with written approval by client of the vendor-suggested standards at a later time.

Privacy Laws: Various state, federal and foreign privacy laws have a wide continuum of harsh to non-existing laws for violators. The 2016 European Union's General Data Privacy Regulation (GDPR)[7] is comprehensive and arguably the most onerous in compliance and penalties in the world, though it is unclear on its extraterritorial application in the U.S. However, should you conduct any international transfer[8] of personal data of an EU natural person, be sure to check the European Commission's newly published standard contractual clauses governing such transfer. In comparison, Canada's privacy laws are less stringent than the GDPR but still more protective than the U.S.'s. Foreign jurisdiction may arise from the physical foreign location of the data. Thus, to avoid triggering onerous foreign privacy laws, if practicable, a contract often prohibits storage, use or processing of such data outside the U.S. In 2018, California led the nation in passing a comprehensive privacy law modeled after the GDPR. Other states[9] have passed or have in the pipeline personal privacy legislation.

Cybersecurity Provisions. The agreement should address key issues such as (a) physical security of the structures in which IT equipment is held, (b) network and internet security protocols, (c) data breach protocols, (d) breach response protocols, (e) disaster recovery, and (f) periodic audit of protocols and updates. Irrespective, cybersecurity standards that your clients have chosen should be clearly agreed to by the vendor along with corresponding remedies. In addition, it could be worth checking to piggyback on a state cloud master agreement. The NASPO ValuePoint, which is the cooperative purchasing arm of the National Association of State Procurement Officials (NASPO),[10] could have new master agreement templates for participating states to use or for your clients to reference. Similarly, the National Chief Information Officers of the States could be a good source of best practices.

Additional Non-Cybersecurity Provisions. Other legal grounds may also restrict unauthorized use, distribution or disclosure of data; including copyright, trade secrets, and Protected Critical Infrastructure Information (PCII) designation.[11] For IT agreements involving utilities (electrical grids, water supply, airports, etc.),

Continued on page 36

it could pay to have client determine the benefits from pre-designating the information as PCII versus the administrative burden.[12]

Therefore, an expansive set of cybersecurity provisions should not only lower the chance of data breach, system hack or even ransomware, but also increase remedies for clients. As fully discussed in Section III above, indemnification is a great tool to recoup damages from vendors.

As a back up to the indemnity obligations, it is common nowadays to require vendors to provide cybersecurity and/or data breach insurance, because cybersecurity insurance policy choices are abundant and costs tolerable. Given the nature of the data in each transaction, risk manager could assist in assigning an appropriate coverage amount so as not to over insure. As in other insurance policies, clients shall be the named insured to capture 100% of the policy benefits.

Finally, cybersecurity or data breach could bring not only financial losses but also bad press to government clients. But appropriate standards and effective provisions could lower the risks significantly.

V. Confidentiality, Public Records Compliance, and Municipal Data Retention/Destruction – Eugene Hsue, Assistant City Attorney, City of Philadelphia Law Department

General Overview: A practitioner must balance a city's liability-free compliance of public records law with a vendor's legitimate business interest in its proprietary information and business secrets. On one hand, the requirements of any applicable public records law constrain any potential obligation of confidentiality that a city may owe a vendor for information flowing from vendor to city. With respect to municipal information flowing to the vendor through its cloud-based service or other means, the municipal attorney should obligate the vendor to a duty of confidentiality, as well as ensure that any requirements mandated by applicable privacy statutes apply. Making a vendor agree to an express acknowledgement of the city's requirements under an applicable public records statute is the practitioner's safest bet. In the language of that acknowledgement or elsewhere, the municipal attorney should disclaim any liability on the city's part that stems from disclosure of public records containing the vendor's documents.

Starting Positions in Negotiation – Pro-City Positions: A city may receive a multitude of the vendor's documents as either part of a RFP response or the city's cybersecurity audit of the vendor's product. With respect to this vendor information, the strongest (and arguably unreasonable) position that a city can take in the first instance is to not owe the vendor any duty of confidentiality. The practitioner should become competent with the category of documents which, under a jurisdiction's public records law, unambiguously fall into the category of being "public records." This category could include large portions of the vendor's RFP response or the resulting contract. If not yet competent, the practitioner should consult with colleagues who specialize in public records litigation. For vendor information that clearly constitutes a "public record," the practitioner should avoid contractual language that obligates the city to keep these documents confidential. Neither should the practitioner countenance any liability attaching to the city for their disclosure.

If the vendor pushes for a duty of confidentiality to attach to the city, then the practitioner should ask the vendor to explain how certain documents constitute business secrets or proprietary information. Reasonable vendor requests may include a vendor's references, which divulge business clientele, or a vendor's cybersecurity audit, which divulge the technical measure by which a vendor keeps its product secure. If a practitioner agrees to such a duty, the practitioner should be sensitive to the administrative implementation of confidentiality: One suggestion would be to require the vendor to emphatically mark in writing those documents as "confidential" or "proprietary."

Municipal information Flowing to Vendors: First, the practitioner should consult with privacy law colleagues or treatises on whether the content of that municipal information triggers legal requirements under privacy statutes. For example, health records of city residents may trigger HIPAA requirements that any recipient of that data become a "Business Associate" of the city's. Transactional attorneys should work closely with privacy law experts to draft boilerplate language that satisfies all of the city's privacy law mandates. In addition to privacy law requirements, the practitioner should consider obligating the vendor to confidentiality of this municipal information. The scope of this duty could include a prohibition against the monetization of this data and against its storage on any third-party's servers (like Amazon Web Services or Sales Force). There does exist the opportunity for the city to collect royalties, either continual or one-time, on the vendor's use of that data. However, in the case of continuous royalties, the city may need to rely on the vendor's platform for these statistics, and there would be no way to independently verify those numbers apart from the vendor. Ultimately, whether or not to collect royalties based on the vendor's use of municipal data is a business decision left up to the client.

Commonly Encountered Vendor Positions: In addition to documents containing proprietary information and legitimate business interests, vendors may aim to enlarge the scope of documents which they seek to obligate the city in keeping confidential. Vendors may propose and argue the RFP response, the overall monetary value of the contract, and the contract itself some-

how constitute "business secrets" or are "proprietary" to them.

The city practitioner should counter the vendor's assertions with a firm understanding of what constitutes a public record under applicable public records law. In negotiations, the city practitioner should inform the vendor that the city's contractual obligation of confidentiality cannot encompass materials which at law are public. Otherwise, that contractual term itself may be void as illegal.

Very often, the vendor may push for the duration of the city's confidentiality obligation to be in perpetuity. Ultimately, this is the client's business decision which implicates the client's technical ability to keep the vendor's information confidential. One suggestion to counter this vendor proposal would be to obligate the client to destroy the vendor's data, to certify that destruction to the vendor by writing, and then for the client's duty to extinguish upon destruction. The city itself may seek for the vendor's confidentiality obligation to be in perpetuity, particularly where health records of residents flow to the vendor. In that case, the city may not want to curtail the duration of the vendor's duty with the vendor's destruction of that data, nor the certification of that destruction. Ultimately, this is a client's business decision.

Vendors often may want to place the administrative burden of identifying which of its documents contain proprietary information or business secrets upon the city. The city should push back, because it simply is not in the best position to understand the vendor's own documents; the vendor knows its business and documents best. The city should require the vendor to identify which documents contain a business secret or are proprietary, by expressly and prominently marking those documents The contract could include a clause obligating the City to notify the vendor if there is a request for disclosure of the vendor's records, but placing the burden of proving those records as exempt from disclosure upon the vendor in the context of public records litigation. The city should not have the burden or expense of protecting the vendor's proprietary information. This is a reasonable cost of doing business with government.

Reasonable Middle Ground: Where city and vendor information flow to one another, well-drafted language should include bilateral confidentiality obligations that balance the vendor's legitimate business interest in its proprietary information with the city's legal obligation to make certain records public. The city should expressly disclaim any potential liability to the vendor resulting from compliance with public records disclosure, and the vendor should acknowledge that the city's public records obligations govern the city's treatment of the vendor's records. On the other hand, to the extent that the city receives the vendor's business secrets and proprietary information prominently marked by the vendor as such, the city should keep that vendor information confidential until the city destroys it, consistent with applicable public records laws.

CONCLUSION

We hope you find this article helpful. If you have any questions, do not hesitate to contact any co-author at the email addresses below. Happy negotiating! ML

NOTES

1. "Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption." <https://www.cisa.gov/>
2. https://www.cisa.gov/ransomware-fact-sheets-and-infographics
3. Global Resilience Federation, InfraGard, ISACs/ISAOs, and NCFTA.
4. Protected Health Information ("PHI") may be defined per 45 C.F.R. §160.103.
5. Personally Identifiable Information ("PII") is generally defined as information that can be used to identify, contact, or locate a natural person, including without limitation, natural person's name, IP address, email address, postal address, telephone number, account numbers, date of birth, driver's license or other government-issued identification card numbers and social security numbers, or any other information that is linked or linkable to an individual.
6. International Organization for Standardization ISO 27001; National Institute of Standards and Technology NIST SP 1800 Series Practical Guide; International Electrotechnical Commission (IEC); British Standards Institution;. Center for Internet Security CIS; Internet Engineering Task Force; System and Organization Controls (SOC 1 & 2); and Payment Card Industry Security Standards Council.
7. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("General Data Protection Regulation," repealing Directive 95/46/EC) (27 April 2016, *effec.* May 25, 2018). *See also,* REGULATION (EU) 2018/1725 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC). (23 October 2018).
8. < https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en>
9. Virginia, Colorado, Illinois, Massachusetts, New York, North Carolina, Pennsylvania and Texas (as of June 11, 2021 per the IAPP State Privacy Legislation Tracker <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/>.
10. https://www.naspovaluepoint.org/portfolio/cloud-solutions-2016-2026/#participants
11.Cybersecurity & Infrastructure Security Agency <https://www.cisa.gov/pcii-program>
12. <https://www.cisa.gov/>