Take It or Leave It: Pitfalls and Challenges of IT Contracts

Thursday, May 4, 2017 General Session; 9:00 – 10:30 a.m.

Margarita Gutierrez, Deputy City Attorney, City and County of San Francisco
Rosa M. Sanchez, Deputy City Attorney, City and County of San Francisco

DISCLAIMER: *These materials are not offered as or intended to be legal advice. Readers should seek the advice of an attorney when confronted with legal issues. Attorneys should perform an independent evaluation of the issues raised in these materials.*

Notes:____

Take It or Leave It: Pitfalls and Challenges of IT Contracts

Prepared by Deputy City Attorneys Margarita Gutierrez and Rosa M. Sánchez- Office of the San Francisco City Attorney.

Special Thanks to Spring Intern - Caitlin B. Wiley, Juris Doctor Candidate 2017 University of San Francisco School of Law, for her assistance with this paper.

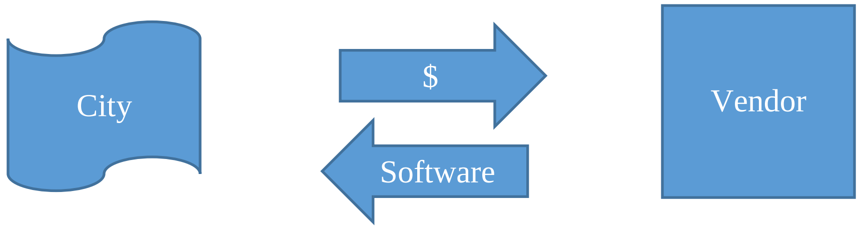
As technology evolves, so must city contracts that cover these transactions. As government attorneys, we need to understand the changing technology we are procuring for our cities in order to negotiate better contracts with these vendors.

The computing systems utilized by most cities from the 1960s through the 1980s involved multiple terminals that were networked to a mainframe located on city premises. During most of this time, the technology was maintained by in-house technology departments, and the information processing was tailored to each city department's individual needs. In the 1990s, the expansion of the internet brought about a new class of centralized computing, called Application Service Providers (ASP). These providers hosted specialized business applications with the goal of reducing costs. Now, hosted services have essentially extended the idea of the ASP model into a software as a service (SaaS) or a "Cloud" computing model.[1]

At its core, SaaS offers the ability to access specialized business applications over the Internet using connected devices. Due to budgetary constraints and the ubiquity of software as a service at much lower prices than an on-premises model, cities are looking more and more into moving their data from an in-house environment to a hosted environment. Following is a discussion of issues cities should consider when moving their data and information processing into the cloud environment.

SAAS-CLOUD TRANSACTIONS

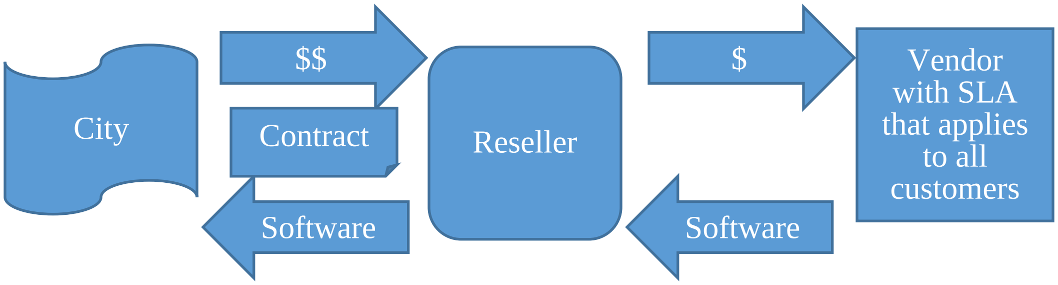
Before the development of the cloud, cities would negotiate directly with a software license vendor to purchase a product that would belong to the city. The city would continue to pay the vendor for maintenance over the life of the product in a series of term-limited agreements. It could include all of its requirements in one agreement with the vendor that would establish service levels, cost and quantities.



In a cloud subscription model, it is more likely that a city will enter into agreements with both a reseller and a vendor. Many technology companies, such as Microsoft and Salesforce, require city wide transactions be done through large account resellers ["LAR's"] and they will not

[1] The National Institute of Standards and Technology defines software as a service as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and releases with minimal management effort or service provider interaction."

contract directly with the cities. The vendor's service agreement may establish the minimum service requirements for all customers and the terms of use for the service. The reseller agreement will integrate the vendor's agreed upon terms and may add payment terms, insurance and additional city-mandated requirements.



Although the reseller may provide some additional services such as training for employees, a help desk, and a first point of contact in case of a problem with the service, the data processing is performed by the vendor. The starting point of such a transaction is figuring out each party's responsibility and how the data will flow. Although vendors will claim that service level agreements cannot be changed, some terms can be negotiated directly with the vendor, especially for large transactions. If a term cannot be changed with the vendor, the LAR may agree to provide an alternative through their agreement with the city. Cities should consider the following issues when negotiating a hosted software agreement.

1. **Sensitivity of data** – What type of data is being transmitted/processed and what applicable federal, state or local regulations apply? Agreements concerning data such as health information, personal identifiable information, credit card information, or whether a person is a public benefits recipient must reflect additional regulatory compliance requirements. For example, agreements that include storing health information should include a Health Insurance Portability and Accountability Act (HIPAA) BAA.[2] Similarly, additional requirements are likely necessary for agreements involving criminal justice information. Even agreements for word processing and email services such as Microsoft O365 agreements may require the inclusion of a BAA in order to protect all parties.

2. **On-line and hosting facility security.** What type of security measures are in place to make sure the city's data is protected and what encryption levels are being used? Is the data encrypted in transit and at rest? What physical security procedures does the hosting

[2] In general, a business associate is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information. Business associate functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review, and billing. *https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulation*

provider follow at its facilities to prevent unauthorized access? The vendor's employees should only access the city's data to the extent necessary to maintain the service.

3. **Ownership and location of data.** Is data ownership clearly defined in the agreement? Where will the data reside? Is the vendor requesting a perpetual license to use de-identified aggregate data to run analytics on the data traffic? Giving vendors the right to use de-identified aggregate data should be carefully considered because individual identities can be reassembled by sufficient manipulation of big data aggregated sets.

4. **Disaster recovery and location of the primary and back up data centers.** What is the vendor's data recovery plan and where is it in the agreement? Identify the location of primary and backup secondary centers, including the city and state, and ensure the agreement requirements flow down to the subcontractor(s). Furthermore, require prior notice and city approval of changes to subcontractors. Finally, consider whether the contract should require the data to remain in the United States to avoid, for example, falling under international data import/export laws. A helpful tool in these transactions is a data map which can help you understand whether subcontractors are involved and where the points of possible breach are.

5. **Availability of data**. The "uptime," or availability to the city's data, is one of the most important aspects of a hosting provider's performance measure. Does the city have 24-7 access to its data? Does, or should, the city keep a copy of the data in one of its own servers? If so, in what format? What happens if the vendor's primary data center is down and the city does not have access to its data for an extended period of time? Does the agreement address this concern by requiring that the secondary data center kick in within a specified period of time? The agreement should address the uptime the city expects through a service level agreement. Uptime is often measured in "nines."[3] Depending on the nines you agree to (99%, 99.9%, 99.99%, 99.999%, etc.) the city's access to its data might be reduced anywhere from 7 hours and 12 minutes in 30 days (for 99% availability) to 3 seconds in a 30 day period (99.9999% availability). No hosting provider can guarantee 100%, but the city should consider which nines are appropriate in each transaction depending on the data the city plans to store in the hosted environment.

6. **Termination provisions and vendor bankruptcy**. What happens if the city wants to change providers or end the service? What happens if the hosting provider declares bankruptcy? On termination or expiration of the agreement, the hosting provider should provide the city with a complete copy of the city's data in an agreed upon machine readable format within a specified timeframe, and require the hosting provider to certify in writing that it will purge all city data from the vendor's servers in a way that the data

[3] https://www.hostingmanual.net/uptime-calculator/#tab-id-1

cannot be recreated.[4] The agreement may require the vendor's assistance in the transition of the city's data to a new service provider, or in-house server. Vendors will most likely agree to assist in moving the data as long as it is at the city's expense. Termination provision can shift the expense of the data transition if the vendor is at fault for the termination.

7. **Audits**. What audit requirements are important to ensure that the vendor is satisfying compliance programs and confirm that management is executing oversight to assure privacy compliance? The city may require a third party auditor to perform a Statement on Standards for Attestation Engagements (SSAE)[5] audit on Controls at a Service Organization (SOC 1/2/3). Audits should be performed on a regular basis and a summary or copy of an SSAE 16 audit report provided to the city.[6] Additionally, agreements should include a city's right to perform an audit of the performance of the services.

8. **Records Retention Policy and Litigation Holds.** What is the city's records retention policy and will the hosting provider be required to comply with the policy? The agreement should address what the city expects the hosting provider do in the event of a litigation hold. At minimum, the agreement should provide that upon notice from the city of a duty to preserve, the provider must save a copy of all the relevant data as it exists up to that date. Suggested language is as follows: "Contractor shall retain and preserve City Data in accordance with the City's instruction and requests, including without limitation any retention schedules and/or litigation hold orders provided by the City to Contractor, independent of where the City Data is stored."

9. **Public Records Requests and/or Subpoenas.** Will the city have access to its data in such a way that searches can be run for existing records responsive to a records request? The agreement should also specify the process to be followed by the hosting provider if it receives a subpoena or other request for disclosure from a third party.

10. **Limitation on Click-Wrap Disclaimer.** The agreement should specify that even if the hosted application has a click-wrap agreement or privacy policy that must be clicked by the authorized user/end user as a condition to gain access to the hosted environment and application, the click-wrap agreement or privacy policy does not apply to the agreement. The agreement should state that only the written provisions of the parties' agreement

[4] Secure disposal shall be accomplished by "purging" or "physical destruction," in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-88 or most current industry standard.

[5] http://ssae16.com/SSAE16_overview.html and http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/SORHome.aspx

[6] SSAE 16 Audits: SOC 1 audit (financial institutions) or SOC 2/SOC 3 (data privacy)

apply to the city's designated users for access. In the event a click-wrap disclaimer/agreement is required for a specific agreement where end users must click through for access to the application, the agreement should state that the city has the right to review and approve such click-wrap disclaimer prior to its implementation.

11. **Disabling Code.** Computer instructions or programs, subroutines, code instructions, etc., may come with programs purporting to do a meaningful function, but designed to time-out or deactivate functions in the application or terminate the operation of the licensed program, or delete or corrupt data. The contract should prohibit the use of such disabling code by the vendor.

12. **Dispute Resolution/Venue.** The agreement should address the steps to be taken in the event of a dispute. Vendors might ask for the right to suspend their services in the event, for example, of a payment dispute. In most cases, this will not be an acceptable provision. Cities should contractually ensure that they will have access to their data at all times, even if a dispute arises with the vendor. Consider establishing the venue for any dispute that arises. The vendor's willingness to negotiate on this issue may be based on the amount of the agreement and the amount of business they do in the State of California.

DATA BREACH CONSIDERATIONS AND REMEDIES

Defining the risks of and responsibility for breaches of data are a crucial element in the negotiation of a SaaS agreement. A wide range of state and federal laws cover data breaches. One important development affecting a city's SaaS agreements is the recent expansion of the California Information Practices Act (the Act) on January 1, 2017 to require breach notification by local agencies.[7] For this reason, the cost of notifying affected individuals has become a significant issue in these agreements.

1. **Data Breach.** The Act defines breach as, "unauthorized acquisition or "reasonable belief" of unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency.[8] The definition of data breach may be incorporated into vendor agreements as the triggering event for loss and response. As the data owner, the city is responsible for notifying affected individuals of the breach in, "the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement."[9] This makes it even more important to evaluate the costs of breach notification when

[7] *Cal. Civ. Code §1798.29(k)*

[8] *Cal. Civ. Code §1798.29 (a) & (f).*

[9] *Cal. Civ. Code §1798.29(a)*

negotiating a vendor SaaS agreement. At a minimum, contracts should require timely notice of a breach from vendors, and insurance that covers the costs of notification from resellers.

2. **Remedies.** Remedies for breach can be one of the most difficult areas of the agreement to negotiate. Cities can request complete unlimited liability (including incidental and consequential damages) and corresponding indemnities for security and privacy breaches, but the vendor is likely to seek a cap to its liability for privacy and security breaches, or any other type of breach. It is critical to understand the number of data records and nature of the data in order to develop appropriate insurance requirements, indemnification language (both general and for infringement), liquidated damages, and any limitation of liability clause, including carve outs. Where the vendor's liability for data breach is capped, it is advisable to negotiate a carve-out for damages arising out of the vendor's willful or reckless misconduct so that the cap will apply only to simple negligence.

3. **Insurance.** Cyber Insurance can help mitigate losses sustained from a data breach, but there is no standard policy language that applies in all cases. Unfortunately, a city's usual practice of requiring comprehensive general liability policies [CGL] for all city vendors may not be helpful in case of breach because these policies are unlikely to cover the cost of notifying affected individuals of a breach of their data, the associated fines or damages and/or malfunctioning systems.[10]

4. **Recovering damages.** Individuals affected by data breach have had a difficult time recovering damages. Because the costs of notification can be so significant, it is still important to carefully craft the cyber coverage to compensate for expenses related to investigation and notification. The SaaS agreement should clearly state how the parties will cooperate with law enforcement, and notify the affected parties. Ideally, the vendor would agree to pay for at least one or two year(s) of credit monitoring services for those affected by the data breach. The agreement should address details of responding to a breach. Which party may speak to the media about or comment on the breach? May a party do so without the approval of the other party? May it name the other party?

Because this is an emerging area of law, older agreements may not contain adequate provisions for data protection. It is a good practice to evaluate existing agreements to make sure you have insurance protection that follows the data and applies to the actual costs incurred for the breach. For example in *P.F. Chang's China Bistro, Inc. v. Federal Ins. Co*, P.F. Chang purchased cyber

[10] See, e.g.,. Zurich Am. Ins. Co. v. Sony Corp. of Am. 6 N.Y.S.3d 915 (N.Y. App. Div. 1st Dep't 2015).Holding that Zurich's CGL policy did not afford Sony coverage for the 2011 data breach of its PlayStation network because the third party hackers, and not Sony published the stolen information.

insurance policy marketed as, “a flexible insurance solution designed by cyber risk experts to address the full breadth of risks associated with doing business in today's technology-dependent world.”[11] After 60,000 credit card records were breached, the chain looked to its insurer for reimbursement of the bank fees charged by its card processing agent. The court found that the charges were properly denied because the insurer “should not be liable for any Loss on account of any Claim, or for any Expense … based upon, arising from or in consequence of any … liability assumed by an Insured under any contract or agreement.” [12]Essentially, since P.F. Chang’s agreement with the card servicer addressed payment for fees assessed for fines, penalties and assessments, the insurer did not have to cover this expense. The decision is currently on appeal.

Although the value of the contract will impact your ability to negotiate the terms, cities have a great asset in these negotiations due to the nature of government contracting. While a vendor may claim the pricing information is confidential, the terms of the agreement will be publicly available, so your fellow City Attorneys may be your best resource. In most cases, a carefully carved out limitation of liability provision and language defining how your city’s data can be processed and used is the key to these agreements.

<u>RESOURCES</u>

California Attorney General’s List of State and Federal Privacy Laws
https://oag.ca.gov/privacy/privacy-laws

California Department of General Services
http://www.dgs.ca.gov/pd/Home/CloudComputing.aspx

NIST Publication
http://csrc.nist.gov/publications/PubsSPs.html#800-145
http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf

SSAE Security Guidance
http://ssae16.com/SSAE16_overview.html

[11] *P.F. Chang's China Bistro, Inc. v. Federal Ins. Co.*, No. 2:15-cv-1322 (SMM), 2016 WL 3055111 (D. Ariz. May 31, 2016).

[12] *P.F. Chang's China Bistro, Inc.* 2016 WL 3055111 at *7.