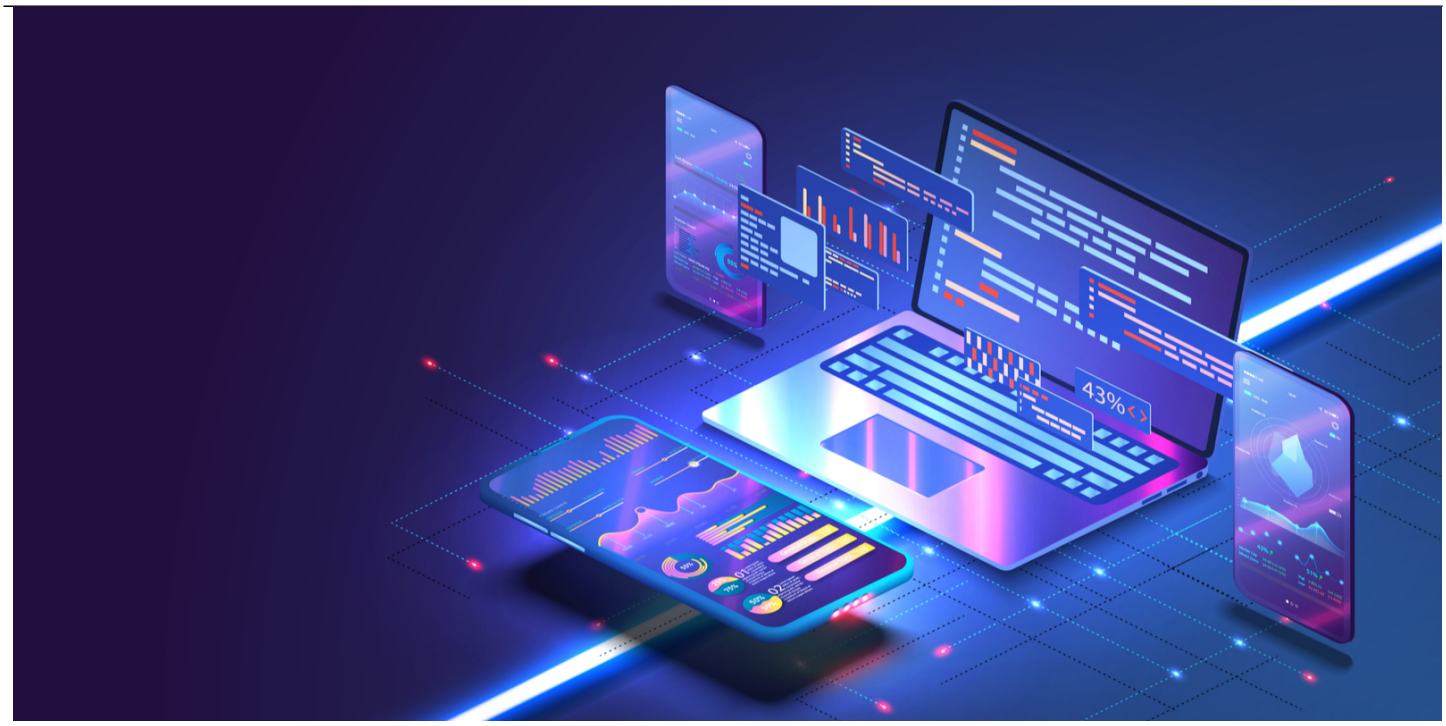
Best Practices for Negotiating Software Contracts

Commercial and Contracts

Technology, Privacy, and eCommerce



Cost, convenience, and acceptance are driving the business world's move to the cloud, and the trend has accelerated during the COVID-19 pandemic. While there can be major advantages to partnering with cloud vendors on software and data storage, it can also expose companies to cybersecurity risks and debilitating outages. Ultimately, you are giving up control in a cloud relationship, and the only thing that protects you is your contract.

For that reason, the negotiation of software as a service (SaaS) and other types of cloud agreements has become extremely important to how software licensees manage cybersecurity risk in their businesses.

By following best practices in negotiating those contracts and collaborating with relevant internal stakeholders, in-house attorneys can help companies maximize the cloud's upside and minimize its downside from a customer/licensee perspective. Outside counsel can provide additional insight on what is generally acceptable in the market and how other companies have dealt with risk.

What's driving the move to the cloud

While the cost savings in capital expenditures may not be as big today as they were 10 years ago, switching to the cloud typically remains less expensive for companies. Instead of buying a perpetual license, they buy a license for a limited subscription term and don't have to pay for servers, electricity, and in-house maintenance. The cost associated with having internal personnel or consultants work on a variety of different systems is also a factor, as a cloud approach is instead streamlined under one central manager of data security.

There is also strong appeal in the convenience that comes with the cloud. Instead of, say, a three-month installation window, companies can often flip a switch and have the full platform live and often accessible by a web browser within a week of signing the contract.

They can easily push out updates. And they can run analytics in real time to see how data is flowing, where security vulnerabilities are popping up, and who is accessing various sources of data. That used to take weeks of IT personnel's time with on-premises solutions. With the cloud, you can access it anytime from commonly supported browsers.

In addition, the cloud is becoming an accepted industry practice. Years ago, cloud-based computing was not considered secure. Now, even consumers are comfortable storing their personal information on the cloud, and businesses face dwindling on-site options. When contracts come up for renewal, licensors frequently say they no longer offer an on-site solution.

The cloud is becoming an accepted industry practice.

How companies can best position themselves in cloud agreements

The biggest downside to the cloud is that if something goes wrong, a business is only as protected as the contract says it is. That's why the negotiation of cloud agreements is so critical.

Companies should first think through the full lifecycle of any cloud relationship. What happens when the software gets updated? Who is implementing the update? What role would that cloud provider play in the transition to the next one if you have to terminate the agreement? Working through those operation-focused details and including them in the contract can really help down the line. While outside counsel digs into the weeds of the contract, in-house counsel can help facilitate discussions between the legal team and the relevant IT professionals who will be using the cloud solution.

Timeline

You also want to be careful about locking in a long-term contract with a new vendor. Vendors will almost always entice you with a lower price if you'll add on more years. But we have had many conversations with businesses who feel unsatisfied with the cloud solution — but are stuck in the contract — when there are several years left in the term.

Lookout for loopholes

It is also important on the front end to evaluate how mission-critical the software is. If it is crucial to the operation of your company, in-house counsel should really scrutinize the service-level agreement to figure out if it provides enough protection from downtime. Many vendors will promise a minimum of 99.5 percent availability, but there are loopholes that allow them to declare a particular outage doesn't count toward that calculation. Diving into the service-level agreement can uncover those loopholes.

Data is the dealbreaker

Another crucial step is identifying and understanding the data elements in the contract. That's often the whole ballgame. The type of data or information at play will dictate how aggressive to be in negotiations.

For example, some companies will be much less willing to give ground in dealing with protected health information versus other types of information. While outside counsel can often provide guidance on the various privacy regulations applicable to the transaction, in-house counsel can provide company-specific knowledge regarding enterprise risk management strategy and internal data management policies.

Stakeholder engagement

Having the business stakeholders heavily invested in the process to explain what data is going to be involved and what the software does is really important. One of the challenges with cloud agreements can be articulating to the business team what these esoteric legal terms mean for them in terms of financial or operational risk, especially when they are pushing to use the software as fast as possible. Approach this as a chance to educate them on how the contract could be bad for your company if it is missing terms that many businesspeople wouldn't even know to add.

In working with the business team, you also want to think about how to quantify the risk. How likely are we to face litigation tied to the EU General Data Protection Regulation (GDPR) or the California Consumer Privacy Act, for example? If the business team wants to enter into a limitation of liability where you can only collect a limited amount of damages in a dispute, can you find examples of what similarly sized companies have had to pay in settlements about that same issue?

Translating the legal risk into something concrete that could come out of next year's budget can go a long way. In-house counsel can provide insight on how frequently the company has taken any particular position in the past, while outside counsel can provide a guidepost for whether the company's position is aligned with the market standard.

It is also helpful to quickly identify other internal stakeholders who will need to comment on draft contracts. If you are using an international software as a service, for example, you may want the privacy officer to review the draft and provide guidance on data privacy implications. You may also run into export control and other international sales legislation, so there may be an internal subject matter expert to consult on that.

> Assembling a team of all the experts on the front end will result in a smoother process and prevent headaches down the road.

Similarly, if your software as a service is functioning in a way that replaces or augments internal employee resources, you may want to have an employment attorney ready to briefly review the agreement and make sure that no additional provisions are required. There may be insurance implications as well.

You get the point. Assembling a team of all the experts on the front end will result in a smoother process and prevent headaches down the road, regardless of whether that team is staffed by the company's internal resources or a law firm's diverse transaction team working together as outside

counsel.

In-house counsel should also develop a clear road map for when to escalate an issue internally and to whom to escalate it. All of these steps should be incorporated into a concrete internal process that your company not only knows about but follows. The process should also be revisited periodically to account for legal and business changes, as well as practical lessons.

Data privacy laws are springing up more globally, and tomorrow there could be a new data privacy law that changes the shape of how to negotiate the next contract.

Final takeaway

If in-house counsel construct thoughtful internal processes and follow them in negotiating cloud agreements, the end result can be better protections, faster turnaround times, and fewer surprises. You want to cover every situation you can so that there is no ambiguity if anything goes wrong. Having a strong working relationship between in-house and external counsel is key.

In cases where businesses do not have the leverage to reach the exact terms they want, there are creative alternatives. It is worth thinking beyond the contract. Whether you are a licensor or a customer, consider how you can mitigate risk operationally in addition to contractually.

If you are unable to get favorable terms regarding one type of data, can you put in physical safeguards to ensure that type of data is never uploaded to that software? Can you train your personnel on basic data privacy principles and make sure they’re aware of the consequences of mistakes?

Those beyond-the-contract steps are obviously imperfect. If something slips through the cracks, you are at the mercy of unfavorable contract terms. But those steps can reduce risks as part of a company’s comprehensive approach to navigating the move to the cloud.

Brandon George

Corporate Counsel

Laboratory Corporation of America Holdings

Brandon George is corporate counsel for Laboratory Corporation of America Holdings. George manages a wide variety of commercial contracting matters with an eye toward managing institutional risk in the areas of privacy, intellectual property, and technology law.

Will Cannon

Partner

Parker Poe

Will Cannon co-leads Parker Poe’s Technology Industry Team, whose services include helping clients negotiate hundreds of sophisticated technology contracts every year. Cannon handles contract negotiations and safeguards clients’ intellectual property rights.

Tiffany Burba

Attorney

Parker Poe

Tiffany Burba is an attorney on Parker Poe’s Technology Industry Team. Burba negotiates and drafts contracts involving cloud software, data sharing, cybersecurity consulting, and other areas at the intersection of intellectual property and technology.