Negotiate Your Next Tech Contract Like a Pro

BRIAN GREGG
McNEES WALLACE & NURICK

▶ **When it comes to outsourcing SaaS and other technology and data services, there are many laws, regulations and other details to consider to avoid buyer's remorse and limit liability.**

As organizations increase their reliance on outsourced technology, in-house legal departments are faced with a deluge of contracts to negotiate. These agreements are dense, sometimes poorly written, and may be full of technical jargon unfamiliar to some attorneys. Deal-focused contract managers do not want to negotiate legal terms. Junior attorneys may not have an adequate background, which should include a mix of intellectual property law, privacy/data security law, and commercial contract law to appreciate all of the issues implicated in a software license agreement, software as a service (SaaS) agreement, or other technology service. Out of frustration or lack of familiarity with the legal and technical issues, attorneys often pass on giving these documents the scrutiny they deserve. Most vendor agreements are, not surprisingly, vendor-friendly; not addressing even just few key sections can leave an organization with buyer's remorse, or worse, significant liability. In this article, we consider the contract terms from the perspective of the buyer. Following the recommendations below will produce an agreement that apportions the risks fairly between the parties.

Who needs to use the technology?

Most vendor contracts start from the position that only the specific contracting entity is permitted to use the software/service. Typical language excludes use or access by third parties. These restrictive terms must be revised if the buyer intends to permit its related corporate affiliates or outside service providers to use the software/service. In such circumstances, the buyer should negotiate the right for its affiliates and any other third-party servicers to use the software/service. The buyer should also make sure any formal definition of "affiliate" aligns with its corporate structure. A good practice is to negotiate the right for affiliates to use the software/service and include them as indemnified parties but not make them formal parties to the agreement. This should reduce the risk that these affiliates could be held liable along with the buyer as a party to the contract. This reduces the exposure to the affiliates but permits them to utilize the software/service.

How is the data managed?

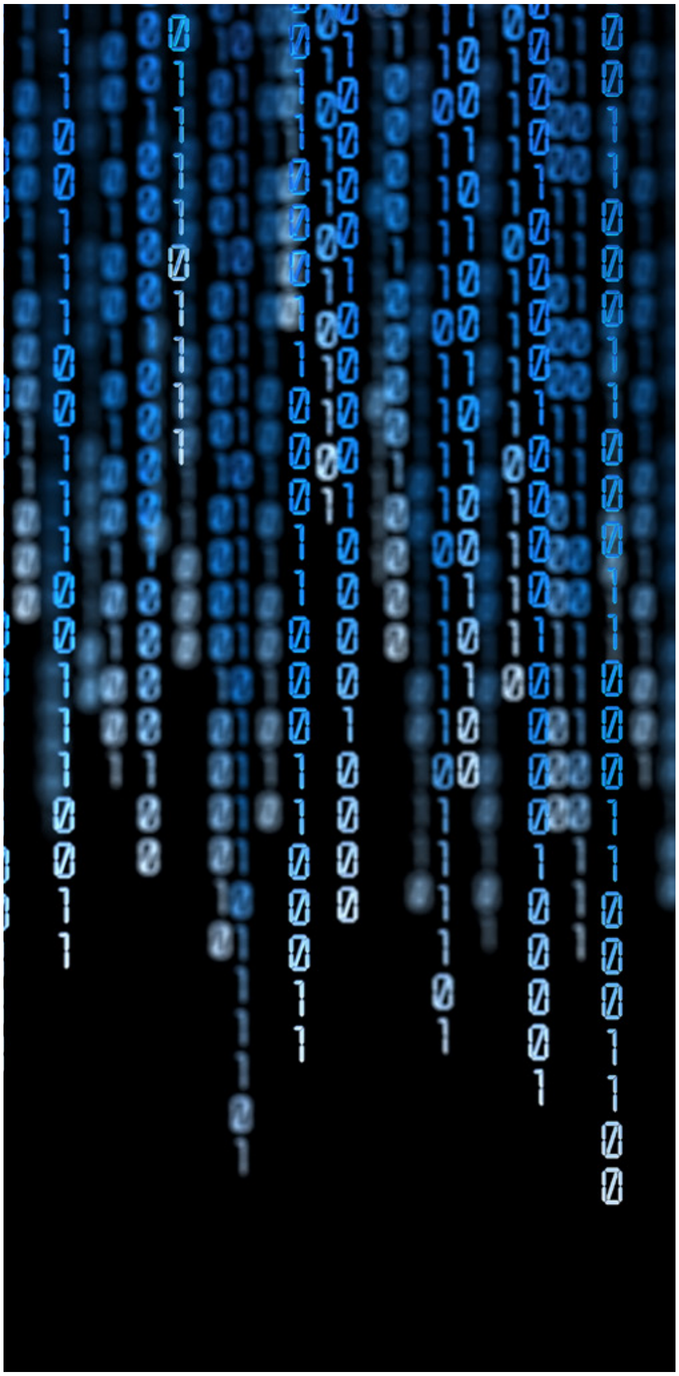
If the engagement involves sharing data, particularly sensitive or valuable data, the agreement must be clear about who owns the data, who owns data generated by the product (data based on data), who can "use" those data sets, and how they can be used. The buyer must ensure that it does not inadvertently give up ownership of its assets, and that it owns any necessary software/service output. Many agreements permit the vendor to own and use "aggregated and anonymized" data, meaning commingled data that is sanitized of its ability to identify a person or entity. Some vendors monetize these data sets. Considerations for buyers include whether the buyer also monetizes its data and is effectively aiding a competitor. Also, buyers should evaluate the privacy law sophistication of the vendor. For example, under the European Union's General Data Protection Regulation (GDPR), personal data only is truly "anonymized" if it's been permanently modified to irreversibly prevent reidentification of the data subject. Under the California Consumer Privacy Act (CCPA), data can be "deidentified." Neither concept is satisfied by merely deleting a field or two from the data set. If companies fail to anonymize/deidentify the data, it may remain subject to the GDPR, CCPA and other privacy laws, and sharing such data may expose the buyer to a claim. A final point on data: Vendor agreements rarely formally address the return of the buyer's data. Buyers should insist on terms that make it clear when and how they can get their data back if the agreement ends or is terminated, regardless of fault.

Confidential information

Most agreements contemplate that the parties will share at least some proprietary information that should be held in confidence. For the vendor, that might be its pricing; for the buyer, that might be its network architecture, future business plans, customer lists, etc. Issues to look out for here include narrow definitions of what constitutes "confidential information," such as requirements that information be literally marked as confidential and that any information communicated orally must be followed up with a written communication confirming its confidential nature. These definitions do not reflect how most organizations treat their data and such a definition undermines the intent of the terms. A better approach to defining confidential information is a reasonableness standard coupled with the usual description of what is not confidential information. Those exclusions usually include (a) information that becomes generally available to and known by the public; (b) information that the receiving party obtains on a nonconfidential basis from a third-party source, provided that such third-party is not prohibited from making the disclosure; (c) information that was known by or in the possession of the recipient prior to being disclosed; or (d) independently developed information. Anther common shortcoming of confidentiality clauses is not imposing a duty to notify the disclosing party if the receiving party learns of its unauthorized disclosure of confidential information.

Confidential information

Most agreements contemplate that the parties will share at least some proprietary information that should be held in confidence. For the vendor, that might be its pricing; for the buyer, that might be its network architecture, future



business plans, customer lists, etc. Issues to look out for here include narrow definitions of what constitutes "confidential information," such as requirements that information be literally marked as confidential and that any information communicated orally must be followed up with a written communication confirming its confidential nature. These definitions do not reflect how most organizations treat their data and such a definition undermines the intent of the terms. A better approach to defining confidential information is a reasonableness standard coupled with the usual description of what is not confidential information. Those exclusions usually include (a) information that becomes generally available to and known by the public; (b) information that the receiving party obtains on a nonconfidential basis from a third-party source, provided that such third-party is not prohibited from making the disclosure; (c) information that was known by or in the possession of the recipient prior to being disclosed; or (d) independently developed information. Anther common shortcoming of confidentiality clauses is not imposing a duty to notify the disclosing party if the receiving party learns of its unauthorized disclosure of confidential information.

SLAs and credits

With any SaaS or hosting service, the buyer wants some assurance that the product will be reliably available. Vendors often address this with a service-level agreement (SLA) in which the vendor promises some level of uptime (usually 99.9 percent), and if the vendor falls short of that target the buyer is sometimes entitled to a credit, often anywhere from 5 to 30 percent of the recurring service fee. It sounds nice in theory, but in practice the credit schemes are often difficult or impossible for buyers to take advantage of and the credit itself rarely approximates the harm caused by an unreliable service. Most SLAs require the buyer to identify the uptime shortfall, which requires the buyer to monitor the service. Most SLAs also require the buyer to request the credit shortly after the excess downtime. Credits of only a few percent of the recurring service fees rarely justify this effort. In addition to the credit scheme, buyers should negotiate a termination right if the promised uptime levels cannot be maintained in several consecutive months or during multiple months over a period of time, such as three months in any rolling 12-month period. The termination right gives the buyer a way to find a higher performing vendor instead of accepting poor performance for the term of the contract. Where possible, the buyer should require the vendor to provide a report on downtime to reduce monitoring needs.

Buyers should insist on terms that make it clear when and how they can get their data back if the agreement ends or is terminated, regardless of fault.

Warranties

A buyer's chief concern is usually that the software/service will meet its needs. That might mean that the software/service offers certain features that provide its value to the buyer, such as being able to interface with the buyer's legacy technology. Without these features, the software/service may be useless to the buyer. Many agreements do not contain any direct statement that binds the vendor to provide promised features. In fact, most agreements contain boilerplate terms that say the opposite – no warranty of merchantability or fitness for a particular purpose. Buyers should override these disclaimers with a clear performance warranty. A typical approach is to require that the software/service work in material conformance with its documentation. This may provide functionality assurance, but only if there is documentation (often there is not, or it only deals with installation) and the documentation includes ref-

erences to the features of importance to the buyer. A more direct approach may be to refer to the description of features in the vendor's proposal or, if not covered elsewhere, include a schedule of critical features that the software/service must offer. Many unhappy buyers will claim that a vendor's product is "broken" when the reality is that the product works as designed but does not do what the buyer desired. Additional specificity in the agreement can help prevent this scenario.

Acceptance and testing

Another concept akin to the warranty issue discussed above is a testing/acceptance process to ensure that the software/service works as promised once it is installed and configured. The buyer should negotiate an adequate amount of time to test the software/service for functionality of any critical features (again, that critical features list can make this process more objective) and for general operability before the software/service "goes live." Ideally, the warranty will not start until formal acceptance, payments are structured to hold something back until formal acceptance and the agreement can be terminated if the vendor cannot achieve formal acceptance. These concepts allow the buyer to retain some leverage after the agreement is signed.

Limit of liability

The limitation of liability and indemnity are the two big risk-shifting terms in the agreement. Most vendor-focused agreements will effectively disclaim all damages except direct damages and will limit the vendor's financial obligation to some function of the buyer's fees. A cap of 12 months of fees paid is typical. This can leave the buyer stuck with liabilities that it assumed were taken on by the vendor, and the vendor with limited exposure. Buyers should consider negotiating a specific dollar cap related to the value of the contract, as opposed to the uncertain "x months of fees paid" formula. The buyer should also push

Most vendor agreements are, not surprisingly, vendor-friendly.

for certain contractual breaches and obligations to be excluded from both the limitations of the types and the amounts of damages. Exclusions typically include breach of confidentiality, breach of data security obligations, indemnified claims, gross negligence, willful misconduct, and other deal-specific terms such as PCI DSS compliance. While less common than negotiating liability caps, it is important to address when damages are limited to direct damages because the outcome of some contractual breaches are foreseeable but are not direct damages. For example, some courts have found that certain damages associated with a data breach are "consequential damages." Vendors have shielded themselves from liability under "standard" contract terms that limit exposure to direct damages and exclude any liability for damages categorized as consequential, special, etc. Buyers must be aware of how newer concerns, like a data breach, might comport with contractual terms often viewed as standard.

Indemnity

The other of the big risk-shifting clauses determines when one party must step in and defend the other against a third-party claim. Some vendor agreements will lack this clause entirely; others may limit indemnification to third-party claims alleging that the software/service infringes a third-party intellectual property right. That is a start. However, buyers should consider other situations where the vendor may contribute to or cause a third party to sue the buyer. These include breach of confidentiality, data breach, personal injury, property damage, and violation of laws such as data privacy laws. As discussed above, if indemnified claims are not excluded from the limitation of liability, the vendor's obligations to defend may not align with the cost of the defense the buyer needs.

Terms via web link

Many software/service agreements contain links to various vendor policies and sometimes entire additional sets of binding terms. Buyers should evaluate whether incorporating these terms, which the vendor unilaterally can change, is appropriate. For example, vendor terms around acceptable use of the service, or certain security protocols, might need to remain flexible so that the vendor can change them to keep pace with evolving laws and security best practices. Buyers need to resist the urge to insist that all such terms be added as formal exhibits and remain static for the life of the agreement, as this may not be practical. However, buyers should be wary of referenced terms that change the major risk-shifting terms of the negotiated document and should consider negotiating a termination right if these "flexible" terms are modified by the vendor in a way that the buyer cannot accept. With a termination right, the buyer retains at least some leverage.

This is by no means an exhaustive list of negotiable terms, but if the buyer considers each of the above issues it will negotiate a more balanced agreement and, in the process, will have thought through the vendor engagement in a more comprehensive manner. ■

Brian Gregg is a member with McNees Wallace & Nurick. He chairs the McNees Food & Beverage Group and is the co-chair of the Intellectual Property Group. Gregg's focus is on trademark and copyright protection, software and technology service contracts, franchising and a number of other related issues. Reach him at bgregg@mcneeslaw.com.