Morgan Lewis

TECHNOLOGY MAY-RATHON

Contract Corner: Annual Update

May 10, 2019

Mike Pierides, London
Peter M. Watt-Morse, Pittsburgh

BACKGROUND

Q&A

Thank you for running in the 2019 Technology May-rathon with us.

We would be pleased to answer your questions.

The Q&A tab is located on the bottom right hand side of your screen. Please type your questions in the space provided and click Send. If we cannot address your question during the live program, someone will reach out to you directly via email with an answer.

CLE Alphanumeric Code

For those seeking CLE credit for this webcast, please note the alphanumeric code read aloud by the presenters. You will need this code to receive a Certificate of Attendance.

An attendance form and survey will pop-up after you exit the webinar.

Please fill out the form and you will be contacted within 30-60 days by our CLE administrative team.

We will process your credits for states where this program has been approved.

For questions regarding CLE requests, please contact Erik Scott at erik.scott@morganlewis.com

INTRODUCTION

Contract Corner

- Tech & Sourcing @ Morgan Lewis Blog:

  https://www.morganlewis.com/blogs/sourcingatmorganlewis

- Contract Corner Feature
- Annual Anthology:

  https://www.morganlewis.com/blogs/sourcingatmorganlewis/2018/12/contract-corner-2018-anthology

- Most Popular Posts

CONTRACT CORNER:

IS IT TIME FOR FORM NDA SPRING CLEANING?

Introduction

- It is important to periodically review form agreements to ensure that the provisions that were favorable or represented your company's position in the past continue to accurately protect your company's interests.
- At the *Tech & Sourcing @ Morgan Lewis* blog, we have given tips on redrafting nondisclosure agreement (NDAs) in the past

  https://www.morganlewis.com/blogs/sourcingatmorganlewis/2015/08/contract-corner-key-considerations-in-understanding-and-negotiating-non-disclosure-agreements
- In this post, we revisited some of those key considerations and expand upon additional items to bear in mind as you review your company's NDAs.

Parties and Term

- At the onset, it is important to identify what parts of a business will use the NDA form and make sure your company's NDA covers each business entity—including your company's subsidiaries and affiliates, if that is the intended scope. Additionally, you should consider whether each entity has the same needs and if those needs can be sufficiently covered in a one-size-fits-all NDA form.
- Consider how long you want confidentiality obligations to remain for both confidential information provided and received, including whether a term is even appropriate when it applies to your trade secret information. It also is important to make sure that your company's NDA dates back to or includes confidential information you may have shared in anticipation of executing the NDA.

Definition of "Confidential Information"

- If you are the discloser of information, you likely want to make sure that the definition of "confidential information" includes summaries and compilations of the confidential information you provide. This, of course, is in addition to other considerations, including whether information can only qualify as confidential under the NDA if it is labeled as "confidential."

Disclosure of Information

- If your company employs consultants that may need access to the other party's confidential information in order to provide services to your company, you may need to include the right for your company to disclose the confidential information you receive to such third party. In exchange for this right, you may need to agree to have in place a commercially reasonable NDA with your consultants and to be responsible, vis a vis the disclosing party, for any breaches of the NDA between the disclosing party and your company arising from any acts or omissions by your consultants.

Standard of Care

- Make sure that your form NDA is consistent with respect to the standard of care that the receiving party must use in protecting the confidential information of the disclosing party. Does the form state that the receiving party will keep the confidential information "strictly" confidential in one place and then state elsewhere that the receiving party will use "commercially reasonable" efforts to protect the confidential information, but not less than the efforts that the receiving party uses to protect its own, similar confidential information? We have seen plenty of forms with this inconsistency.

Obligation to Report Misuse

- If the other side discloses your company's confidential information in violation of the NDA, or the confidential information is otherwise accessed by an unauthorized third party, such as in a data breach, what reporting obligations does the other party have? Must they cooperate with your company in responding to data breaches? Your NDAs should cover these situations to help protect your information and satisfy obligations to other parties in the event of misuse or wrongful access.

Return of Confidential Information

- Depending on the relationship between the parties, the business transaction, and your company's data storage practices, the other side may be the only party with some of your company's confidential information at the end of the term. As such, and in order to prevent the other side from continuing to use your confidential information, your company's NDA should require the return or destruction, at your company's direction, of all of your company's confidential information at the end of the term. This requirement also should cover all copies and summaries the other side may have.

CONTRACT CORNER:

DATA SAFEGUARDS IN SERVICES AGREEMENTS

Introduction

- Drafting and negotiating the data protection provisions in services agreements can be one of the trickier and more time-consuming aspects of the contracting process. One of our prior Contract Corner series from 2014 discussed the importance of documenting security requirements and monitoring security commitments, addressing security incidents, and key issues to consider when drafting liability provisions. In this Contract Corner, we revisited some of these issues based on the latest contracting trends that we are seeing for services agreements and dive into additional considerations when addressing key data safeguard provisions.

Assess and Define the Data

- At the outset of the contracting process, it is important for the deal team and the key stakeholders to evaluate and properly define the types of data that the service provider will access or process as part of the services. A sound understanding of the scope of data involved in a services transaction helps establish expectations up front and will drive a contract that contains the right level of security requirements and an appropriate allocation of liability for security breaches. The contract should then reflect the output of this internal assessment through carefully crafted defined terms that will flow throughout the data safeguard provisions.

Mapping data types and use

- Key issues to consider include:
  - Scope and type of data
    - Client / Client Group / End Customers
  - Jurisdictional origin of data
    - Data residency requirements
  - Data flows
    - Transfers and access
  - Who has access
    - Subcontractors

Assess and Define the Data

As part of the data assessment and initial drafting of definitions, consider the following:

- **Assessing the Scope and Types of Data**: What types of company data will the service provider process or otherwise have access to as part of the services? Is there confidential or proprietary business information involved? Will the service provider have access to personal data, such as data of employees, customers, or other individuals? How sensitive is the personal data? Certain additional requirements may apply if protected health information, payment card data, or personal data of European residents are in scope.

Assess and Define the Data

- **Defining Company Data**: Consider starting with a broad definition of company data, to include all company data and information provided by or on behalf of the company to the service provider or its representatives in connection with the services. Be sure to include personal data within this definition, if applicable, so that such data is afforded at least the same protections under the agreement and, as between the company and the service provider, such data is owned and controlled by the company.

Assess and Define the Data

- **Defining Personal Data**: As with company data, consider defining personal data as broadly as possible to capture any data or information that identifies an individual or that can be used to identify an individual. Try to avoid tying the contractual definition to statutory or regulatory definitions, as such definitions may be designed to trigger notification requirements and thus require some combination of data elements. In addition, clarify that personal data can be in any media or format, including electronic or written records. Also consider if any specific categories or examples should be included based on the services being provided, such as IP addresses or benefits information.

Retain Ownership and Control of the Data

- To help ensure that company data remains "safe" with a service provider, contractual provisions regarding ownership, control, and access to the data should not be overlooked or forgotten. Below we discuss some key concepts to consider.
- **Ownership**: The contract should clearly state that, as between the company and the service provider, all "company data" (as defined) is and shall remain the property of the company and shall be deemed the company's confidential information. As with other intellectual property, consider adding a present assignment of rights (if any) in such data from the service provider back to the company.

Retain Ownership and Control of the Data

- **Use Rights**: After establishing clear ownership rights, consider what use rights the service provider requires to provide the services under the agreement. Consider the following:
  - Include a provision that, without company's approval (in its sole discretion), the company data shall not be used by the service provider other than as necessary for the service provider's performance under the agreement and solely in connection with providing the services.
  - In addition, the contract should expressly restrict the service provider from commercially exploiting the company data and from disclosing, selling, assigning, or otherwise providing the data to third parties without the company's consent.

Retain Ownership and Control of the Data

- Some service providers may be interested in using a service recipient's data (or components thereof) in aggregated and de-identified form for the purposes of improving its services. Consider whether your company will allow this right and whether additional restrictions should be added to the contract, including that the service provider shall not reverse engineer, combine, anonymize, de-identify, aggregate, or commingle any company data. If aggregated data use is permitted, be sure to make clear that such data must not permit the identification of the company, its data, or any of its confidential or proprietary information (including employees and customers).

Retain Ownership and Control of the Data

- **Access and Return**: Retaining access to data is critical, both during the term of the agreement and upon expiration or termination. The contract should address the following:
  - Upon the company's request at any time, the service provider should be obligated (at no charge) to promptly return the company data and/or provide access to the company data, in the format and on the media requested by the company.
  - In addition, the service provider should be obligated to erase or destroy all or any part of the company data in its possession upon request by the company.
  - The service provider should be responsible for developing and maintaining procedures for the reconstruction of lost company data in its possession or control, and should be obligated to correct or restore any lost, destroyed, or altered data in its possession or control at no charge.

Retain Ownership and Control of the Data

- **Retention**: Proper retention of company data is another critical component of data protection. As part of the services, the service provider should be obligated to assist the company in meeting the company's legal obligations with respect to the retention of data and records in the service provider's control. Consider whether the service provider must follow the company's record retention policies or if the service provider's policies are sufficient for this purpose.

Retain Ownership and Control of the Data

- **Legal Holds**: Building on the general retention obligations of the service provider, consider whether the data at issue could be subject to a legal hold that would require cooperation and assistance from the service provider. If, for instance, certain data will be hosted and backed up by the service provider, then the company may require assistance in complying with litigation holds. Appropriate contract language should be added to set forth the process for notifying the service provider of a legal hold and the service provider's commitments with respect to any such legal hold, such as preservation and/or access of the data and the expected time period for the hold.

CONTRACT CORNER:

GDPR AND DATA PROCESSING ADDENDUMS

Introduction

- Although the EU's General Data Protection Regulation (GDPR) has been in force for nearly a year, some organizations are still finalising their implementation of GDPR's requirements, including ensuring that their contracts comply with Article 28, which mandates a number of key clauses if personal data is being processed under the service agreement.
- With potentially hundreds of in-scope contracts, customers and suppliers alike have developed standard-form data processing addendums (DPAs) or similar contract documents in order to address these Article 28 requirements.
- DPAs are fast becoming the preferred approach for both new agreements and existing contracts.

Beware the Order of Precedence Clause

- An almost universal feature of standard-form DPAs is the "order of precedence" clause. This takes a number of forms, but in general it states that in the case of a conflict between the contents of the DPA and the remainder of the contract, the DPA prevails.
- Sounds sensible given this is a regulatory requirement, right? Not necessarily—this approach can undermine, in one fell swoop, what are often highly negotiated and considered provisions in the remainder of the agreement. Article 28 clauses cover important topics such as information security, subcontracting, service locations, and audit rights, and DPAs are often drafted to reflect the minimum obligations mandated by the GDPR.

Beware the Order of Precedence Clause

Let's consider the example of a subprocessor appointment:

- Many organizations (particularly those in heavily regulated sectors) want to retain control over their supply chains, especially where a supplier will have access to or generate customer and other personal information.
- With the continued march of cloud-based, commoditized services, those discussions have become increasingly complex. Indeed, many providers are highly reluctant to agree to a veto right on the use of subcontractors due to their "one to many" business model. The GDPR acknowledges this situation and provides for a minimum approach to the appointment of subprocessors that permits blanket authorizations to appoint subprocessors, provided that processors give notice of changes and additions along with a right for the controller to "object."

Beware the Order of Precedence Clause

- It's no surprise that a significant proportion of providers (in particular providers of cloud-based subscription services) have followed the minimum GDPR approach in their DPAs. Note, though, that many have also included explicit termination rights where a customer objects to a new subprocessor.
- The inclusion of objection processes and termination rights all sounds reasonable, until one revisits the underlying agreement only to find rights of preapproval for subcontracting; those hard-fought positions are swiftly decimated by a combination of the precedence clause explored above and a cookie-cutter approach to preparing the DPA form.

So What Can You Do to Resolve This Situation?

Potential solutions include the following:

- The most important (and obvious) precaution is to read the underlying contract. What does the agreement already say about security, subcontracting, audits, and other relevant items? Are important restrictions and obligations in the wider agreement being inadvertently amended by the DPA?
- Ensure that provisions dealing with similar subject matter dovetail. For example, if there are specific security obligations agreed elsewhere in the agreement in relation to data processing, these should be referenced in the DPA, even if these are called out as "additional" to the standard GDPR security wording.

So What Can You Do to Resolve This Situation?

- Take a more nuanced approach to the order of precedence clause. For example, the DPA might generally take precedence, but certain provisions in the agreement could be stated to take priority. These exceptions could be general (e.g., provisions that are more protective of the customer's information) or specific (e.g., the section that governs subcontracting).
- The DPA is not merely a boilerplate attachment or a rubber stamp to be "GDPR compliant." Make sure the precedence clause, and all other key issues, are in order.

CONTRACT CORNER:

INTELLECTUAL PROPERTY OWNERSHIP – DEFAULT LAWS

Introduction

- Protecting intellectual property rights is a critical component to the success of a technology company. In order for a tech company to determine how to protect its intellectual property, the company should understand how the key intellectual property rights work. In our Contract Corner post, we discussed how patent, copyright, and trade secret ownership works in the United States if there is no agreement in place to allocate these rights. With Mike on board, we will also discuss how the US differs from other countries

Patents

- Patents are a right to exclude others from using a technology for a limited period of time. In exchange for these rights, the patent holder must disclose the invention in the patent. Without an agreement in place to state the ownership of an invention that is patented, the following applies:
- Sole Ownership. In general, the inventor owns the right to patent the invention, regardless of the type of technology. This is the case even when the inventor is an employee who created an invention within the scope of employment

Patents

- Joint Ownership. Occurs when there is more than one inventor (employee from Company A and employee from Company B, for example) or rights have been assigned to more than one person or entity. Even a small percentage ownership or minor contribution results in joint ownership right in the patent. Any owner may exploit a patent either by licensing to a third party or practicing the patent without permission of or accounting of profits to any other owner
- Enforcement. All owners must participate in an enforcement claim. Therefore, if a company jointly owns a patent and wants to file an infringement claim against a third party, all other owners must also agree to file the claim

Copyrights

- Copyrights are a way to protect original works of authorship fixed in a tangible medium, including software code. A copyright is created the moment the work is fixed in a tangible medium. It does not need to be published or registered. (See here for copyright FAQs.) Without an agreement in place, copyright ownership is allocated as follows:
- Sole Ownership. The creator of software or other works is presumed to own the copyright rights to those works. However, unlike with patents, an employer automatically owns copyrights created by an employee in the course of employment. On the other hand, contractors will generally retain ownership of the copyright in works they create and not the party that retained (and/or paid for) the work.

Copyrights

- Joint Ownership. Occurs when (a) more than one creator contributes and there is an intent to combine the individual contributions into inseparable or interdependent parts, or (b) rights have been assigned to more than one person or entity. Any owner may exploit a copyright either by licensing to a third party or using the rights granted under copyright laws without permission of any other owner. However, unlike patents, copyright owners must account for profits and give other owners their share.
- Enforcement. Only one owner is required to participate in a claim (but a license from another owner would moot the claim).

Trade Secrets

- Trade secrets are typically considered to be information that are, or may be, economically valuable because they are not generally known or easy to figure out, and that are the subject of reasonable efforts to keep the information confidential. Trade secrets are typically governed by state common law (rather than the federal statutes that govern patent and copyright law) and therefore, the rights can vary from state to state. In general, if any trade secret is disclosed in a manner that does not protect its confidentiality, the party that owned the trade secret will lose all intellectual property protection for that trade secret.
- Sole Ownership. Generally, the creator(s) of a trade secret (or their employers) own a trade secret. This can (and frequently is) clarified by confidentiality agreements

Trade Secrets

- Joint Ownership. Similar to ownership of other intellectual property, joint ownership occurs when there is more than one creator or rights have been assigned to more than one person or entity. Joint ownership may increase the likelihood that a trade secret will not be properly protected. It is likely that all owners need to account to the other owners for profits
- Enforcement. It is unclear whether all owners need to participate in a misappropriation claim. In addition, whether or not to enforce a misappropriation claim is not as straightforward as enforcing a patent or copyright infringement claim because of the possibility that litigation could make the trade secret information generally known

CONTRACT CORNER:

IP INDEMNIFICATION

Background

- IP indemnification clauses are the most common indemnification provisions in contracts because typically, both parties need the provision. Users of technology licensed or otherwise received from another party will demand that technology providers take care of any third party IP claims that would prevent (or increase the cost of) use of the technology. On the other side of the transaction, IP owners will want to control any IP litigation against their technology and avoid users settling such claims and giving up valuable IP rights (and it is likely the owner is already facing such IP claims directly). Although the provisions are common, the language of these provisions can impact the relative risks of IP litigation between the owner and user. In this Contract Corner post, we reviewed issues related to the defense and indemnification aspects of these provisions.

Responsibility to Defend

- As described above, an IP indemnity clause typically includes the obligation to defend against third party IP claims. However, the potential costs and risks associated with this obligation can be impacted by the language of the provision. For example, do intellectual property rights include IP rights on a worldwide basis or does the owner limit defense obligations to US patent and copyright rights (where the owner does not operate outside of the United States or provide any trademarks or confidential information)? Second, do defense obligations include the right to select counsel and if users retain their own counsel, who pays for such counsel? Third, is the decision to settle any IP claim solely up to the owner or can users prevent settlements that impact their rights or costs for using the IP?

Responsibility to Defend

- One specific word highlights the questions raised by the language of the defense obligation. Typically, these provisions will include obligations that the user must notify the owner of any claim and provide assistance to the owner with the IP litigation. In addition to questions of the timing of such notice or the responsibility for the costs of such assistance, if the language reads that the owner will defend "provided that" the user meets such notice and assistance obligations, the owner may get out from its defense (and/or indemnity) obligations if the user fails to meet these requirements.

Indemnification Responsibilities

- Like any indemnitee, the user will want indemnification for IP infringement to be as broad as possible, including any losses, costs, damages or expenses whatsoever sustained by virtue of the third-party claim. On the other hand, the owner will want to limit the potential indemnification to the damages (or settlement amounts) that are awarded against the user to avoid issues regarding consequential or other damages. Like any indemnification, the decision of who will bear this business risk will largely be a matter of negotiation (and leverage).

Indemnification Responsibilities

- In summary, although IP indemnification provisions are common, the actual language of the provision can impact the allocation of risk for defense and indemnification costs between the IP owner and user. In Part 2 of this two-part series, we will discuss how exceptions, remedies, and liability limitations further impact the allocation of risks from third party IP claims.

CONTRACT CORNER:

IP WARRANTIES VS. IP INDEMNIFICATION

Contract Corner: IP Warranties v. IP Indemnification

- A frequent point of contention between parties negotiating the allocation of risk related to intellectual property rights in connection with the acquisition of intellectual property is the interplay between the warranty and indemnification sections. In this Contract Corner post, we broke down what to look for in these sections and how minor changes in the language can significantly change the rights a party is granting or receiving.

Intellectual Property Warranties

- An intellectual property warranty generally provides that the intellectual property rights being licensed or assigned constitute all intellectual property rights owned or controlled by a party prior to the effective date of the transaction, and that those rights are all the rights necessary for the conduct of the business (as it is currently conducted) after the effective date of the transaction. A warranty may also go on to say such intellectual property does not infringe third-party intellectual property rights. The following versions of this clause demonstrate how this clause can be worded to strengthen or weaken the warranty.

Intellectual Property Warranties

Warranty Provider Favorable

- Party A represents and warrants to Party B that to Party A's knowledge as of the effective date, the intellectual property being transferred or licensed constitutes all the intellectual property owned by Party A with respect to which and to the extent to which, and subject to the conditions under which, Party A has the right to grant or cause to be granted licenses to Party B that are necessary for the conduct of the business of the company as it is conducted as of the closing date (Party A IP), and the Party A IP does not at the time of the transaction violate or infringe any third-party intellectual property rights in the United States.

Note: The warranty above is limited by (1) knowledge, (2) ownership, and (3) the extent to which Party A has the right to grant the rights.

Intellectual Property Warranties

Warranty Receiver Favorable

- Party A represents and warrants to Party B that the Party A IP constitutes all the intellectual property rights necessary for the conduct of the business of the company as it is conducted as of the effective date, and in the usual, regular, and ordinary course of business, and that the company has all intellectual property rights to operate its businesses in the ordinary course of business after the effective date, and the Party A IP will not infringe upon or violate any US or foreign patent or copyright, misappropriate any trade secret, or violate any third party's intellectual property right.

Intellectual Property Indemnifications

- An intellectual property indemnification generally provides that the assignor of the intellectual property rights being licensed or assigned will indemnify the assignee if the intellectual property infringes a third party's intellectual property rights. The following versions of this clause demonstrate how this clause can be worded to strengthen or weaken the indemnification obligations.

Intellectual Property Indemnifications

Indemnitor Favorable

- Party A shall, for [a certain period of time] following the effective date, indemnify, defend, and hold harmless Party B from and against (a) any and all claims, suits, actions, proceedings, or allegations brought against Party B by a third party that any of the Party A IP is invalid; or (b) any and all Losses arising out of any inaccuracy of the representation or breach of the warranty, in each case set forth in the intellectual property warranty.

Note: The indemnification above is limited by (1) time, (2) ownership (because it refers back to the definition of Party A IP (which is limited), and (3) the warranty language.

Intellectual Property Indemnifications

Indemnitee Favorable

- Party A shall indemnify, defend and hold harmless Party B, its Affiliates, and their respective officers, directors, and employees (collectively, the Party B Indemnified Parties) from and against (a) any and all claims, suits, actions, proceedings, or allegations brought against the Party B Indemnified Parties by a third party that any of the Party A IP is invalid or infringes, misappropriates, or otherwise violates the intellectual property rights of a third party; or (b) any and all Losses arising out of any inaccuracy of the representation or breach of the intellectual property warranty.

'Equivalent' Provisions

- Watch out for the explanation that an indemnification gives a party equivalent rights to a non-infringement or intellectual property sufficiency representation and warranty. These provisions can only be considered "equivalent" if they actually cover the same things (e.g., if a party is only indemnifying for intellectual property infringement, and the definition of intellectual property does not cover all applicable intellectual property, the other party would still need the intellectual property sufficiency representation and warranty).

CONTRACT CORNER:

KNOWLEDGE QUALIFIERS IN IP REPRESENTATIONS AND WARRANTIES

Background

- In most transactions involving the sale or license of intellectual property, a buyer or licensee will request that a seller or licensor represent and warrant that such intellectual property does not infringe or misappropriate the intellectual property rights of a third party. This representation and warranty is often heavily negotiated in a license or purchase agreement because the seller or licensor wants to limit its obligations for breach of this representation to limit its liability under the agreement, whereas the buyer or licensee wants to keep this provision as broad as possible to ensure that it receives appropriate protection from third-party claims for the intellectual property it licenses or buys.

Knowledge Qualifiers

- One way for a seller or licensor to limit its obligations under this clause is to qualify the IP representation and warranty to its "knowledge." If a buyer or licensee agrees that the IP representation and warranty can be qualified by the seller's or licensor's knowledge, it is important for the parties to delineate the scope of such knowledge. Knowledge can be limited to actual knowledge, which is information that the seller or licensor actually or consciously knew about, or constructive knowledge, which is knowledge that a prudent individual should have under the circumstances (i.e., information that the individual would be expected to learn after some reasonable level of diligence, or information the individual would be expected to know based on his or her capacity as a director, officer, or employee of the company). Often, the definition of "knowledge" in an agreement will include both the actual and constructive knowledge of certain individuals who have control over and knowledge of the relevant facts.

Application to IP Rights

- In addition to defining the scope of knowledge, from the buyer's or licensee's perspective, it is important that the knowledge qualifier should only apply to certain types of intellectual property. For certain types of intellectual property rights, such as patents and trademarks, infringement liability attaches regardless of whether the accused infringer knew that the intellectual property at issue was protected by the intellectual property right. Therefore, one can be liable for infringing a patent without knowing it exists. Therefore, it is not unreasonable for a seller or licensor to knowledge-qualify its representation and warranty as to patents and trademarks.
- However, in order to prove infringement of a copyright or misappropriation of a trade secret, the intellectual property owner must prove that the alleged infringer actually copied the work for copyright infringement or wrongfully acquired the work for trade secret misappropriation. Because of the inherent requirement for knowledge and access for copyright infringement and trade secret misappropriation, it is reasonable for a buyer or licensee to insist that the IP representation and warranty should not be knowledge-qualified as to copyrights and trade secrets.

Example – Balanced Respresentation

- The company owns or possesses sufficient legal rights to all company intellectual property necessary for its business as now conducted and as currently proposed to be conducted without any violation or infringement of the rights of others, provided however that the foregoing representation is made to the company's knowledge with respect to third-party patents, patent applications, trademarks, trademark applications, service marks, or service mark applications.

Final Considerations

- Depending on the type of transaction (e.g., a knowledge qualifier for patents and trademarks is more common in an asset purchase or M&A deal rather than a technology license deal) and the negotiating leverage of the parties, knowledge qualifiers for IP representations and warranties may be appropriate for facts or matters that are outside of the seller's or licensor's control. However, in all such cases, counsel must carefully craft the definition of knowledge and decide which types of intellectual property such knowledge qualifier should apply.

CONTRACT CORNER:

SUBCONTRACTOR APPROVAL

Background

- Nearly every form of service agreement contains a provision restricting the ability of one or both parties to subcontract their obligations. A typical provision (with a standard quick and dirty markup) might look like this:

  – "Vendor shall not subcontract any of its obligations under this Agreement without the express prior written consent of Customer, which such consent shall not be unreasonably withheld. The subcontractors set forth on Schedule X are hereby approved by Customer."

Issues

- These limitations are often included as a standard part of the legal boilerplate without much thought, but can present significant problems, especially given the broad use and incorporation of third-party technologies and services.

- Consider, for example, a typical software as a service platform vendor. It is likely that the platform vendor uses (1) a hosting provider to serve its application; (2) a call center to assist with customer service; (3) security and penetration testing firms; (4) independent contractor software developers; (5) a marketing and graphics design firm; (6) fraud prevention vendors; and (7) payment processors, just to name several "subcontracted" aspects of a typical platform.

Approval?

- Sometimes, the party asked to make the promise just ignores the restriction and carries on, hoping that there is never an issue. Or, perhaps, the party will list a few of its major subcontractors that it feels are important enough to list, ignoring more mundane subcontractors. Rarer still, the party might drop in a very expansive list of every contractor it uses, so as to avoid a foot fault. Almost never is the list updated in any meaningful way after execution, and almost never is there any real thought from the counter-party doing any diligence on the subcontractor list.

Material Subcontractors

- In today's environment, overbroad subcontracting restrictions seem to be more of a headache than something that offers any real protection. One solution is to be more thoughtful about the restriction, and craft it in a way that is both limited enough that it doesn't pick up contractors that are truly ancillary to the transaction, yet is still broad enough to mitigate risks that are actually appropriate to the transaction.

- If your organization is routinely arguing about the disclosures to make in a subcontracting provision, consider a "**Material Subcontractor**" style provision that provides some thought into the types of approval rights that make sense.

Example: Material Subcontractor Defintion

- Vendor may not subcontract, without the prior written consent of Customer, to a third party any of the following activities (a "Material Subcontractor"):

  a. the provision of a significant portion of the Services;

  b. any use, hosting, or having more than incidental access to, any Customer Data;

  c. any portion of the Services subject to a regulatory framework; or

  d. the development of any intellectual property.

- These categories are not intended to be exhaustive, and different organizations may care more about certain types of subcontractors than others, but the notion that a subcontractor restriction might be narrowed to become more meaningful and reasonable could be helpful if you are having problems in negotiations.

Biography

Mike Pierides
London, UK
T +44.20.3201.5686
E mike.pierides
@morganlewis.com

Mike Pierides' practice encompasses a wide breadth of commercial and technology transactions. Mike advises on major outsourcings, strategic restructurings following divestments or acquisitions, and technology-specific transactions such as licensing and "as a service" arrangements. He is also active advising on new technologies such as blockchain and artificial intelligence.

Biography

Peter M. Watt-Morse
Pittsburgh, PA
T +1.412.560.3320
E peter.watt-morse@morganlewis.com

Peter M. Watt-Morse, one of the founding partners of the firm's Pittsburgh office, has worked on all forms of commercial and technology transactions for more than 30 years. Peter works on business and intellectual property (IP) matters for a broad range of clients, including software, hardware, networking, and other technology clients, pharmaceutical companies, healthcare providers and payors, and other clients in the life science industry. He also represents banks, investment advisers, and other financial services institutions.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore
Tokyo
Washington, DC
Wilmington

Morgan Lewis

*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

THANK YOU