Technology & IP Forum: Technology Agreements – Staying Ahead of the Curve with Checklists and Practice Pointers for Numerous Important Issues

Alan Fishel  
Partner  
Arent Fox  
Washington, D.C.  
Office: 202-857-6450  
alan.fishel@arentfox.com

Robert Gurwin  
Chief Counsel  
Oath Inc.  
Dulles, VA  
Office: 703-265-4196  
robert.gurwin@oath.com
Some Core Issues in Tech and IP

- Warranty
- Limitation of Liability
- Indemnity
- Payment
Warranty

• Technology agreements often include a warranty provision that is designed to protect customers from receiving services, software and/or deliverables that are defective or not in conformance with what the parties agreed to in the applicable agreements and/or the documentation.

• A provider generally wants to provide a warranty that is limited in duration and scope, and under which customers have a limited remedy where the provider fails to comply.

• Limits on the Warranty
  • Duration
  • Scope
    • Extent of Compliance
    • Third Party Materials/Technology
    • Knowledge
  • Remedy
    • Repair
    • Replace
    • Refund
Limitation of Liability

Each party will seek to limit its liability to the other party, but to the extent that any limitations on liability are mutual, each party will need to weigh the risk versus the benefit of agreeing to a higher versus lower dollar amount of liability (e.g., of the two parties, who is more likely to breach the agreement and cause damages)

• Consequential Damages v. Direct Damages
• Per Claim/Aggregate/Hybrid
• Some Common Carve Outs
  • Indemnity
  • Confidentiality
  • Data Privacy or Security Breaches
  • IP Violations/Infringement/Restrictions
  • Gross negligence, willful misconduct, personal injury, death
  • Fees Payment
Indemnity

Some considerations from the Customer perspective:

- the technology infringes on or violates the IP or other proprietary rights of any third party
- breaches of any of provider’s data security or data privacy obligations or other data-related obligations
- claims brought by a provider’s contractor or agents
- breaches of the agreement by a provider
- violations of law by a provider
- acts or omissions of a provider

As a customer, require the vendor to provide documented security principles to which it must abide, and at the very least tie a duty to indemnify to cases where the principles were not followed
Indemnity

Some considerations from the Provider perspective:

• IP limitations
  • only certain IP claims (e.g., copyright and trademark but not patent)
  • only IP rights existing as of the effective date of the agreement
  • only IP rights in certain territories (e.g., the U.S. and Canada)

• IP exclusions
  • customer fails to stop using the technology after receiving notice of the infringement
  • customer is not using the provider’s most current technology (e.g., the most current version of the applicable software)
  • “combination” or “misuse” claims (e.g., a claim that would not have occurred but for the combination of the provider’s technology with third-party technology)
  • caused by or arises from any materials (including information) provided by customer to provider (e.g., to complete a deliverable)

• Liability associated with data breach or loss
  • Many providers do not let a customer turn them into the customer’s insurance company/deep pocket by pushing off all of the exposure for a data/security incident
Indemnity

Some considerations from the Provider perspective:

- Many providers seek to have their customers indemnify them for some or all of the following:
  - IP infringement of third-party rights arising from the customer data or customer technology
  - Violation of any restrictions set forth in the agreement (including in any terms of use)
  - Violations of applicable law
  - Any acts or omissions of a customer’s users

Customers will often push back on most, if not all, of the foregoing. When customers agree to indemnify, it is ordinarily in connection with IP infringement.
Payment

Payment models vary across the different types of technology agreements

Some payment models include:

• Software license fees – upfront and/or recurring fees for support and maintenance

• Cloud services customers – recurring subscription

• Professional services – time and materials or fixed
Payment

• What triggers payment obligations
• Rights to increase fees?
• Potentially “hidden” charges, if any
• Caps?
• Disputing fees
• Rights to terminate or suspend services or provision of deliverables as a result of non-payment
• Audit?
Some Core Issues in Cloud Services Agreements and/or Software License Agreements

Data Privacy and Security
Service Level Agreements
Audits
License Grants
Termination/Suspension
Terms of Use/Privacy Policy
Modifications
Data Privacy and Security

Who

What

Where
Data Privacy and Security

With respect to the Three W’s, agreements often cover:

• Access limitations
• Training and background checks
• Disclosure limitations
• Use limitations
• Compliance with law (e.g., FERPA, HIPAA, GLB)
• Security/Encryption
• Geographic limitations
Service Level Agreements

Common Errors with respect to SLAs:

- Triggering events unclear
- Charts/tables without clear legal ramifications
- Remedy (or lack thereof)
- Unclear exceptions

Provider’s generally want certain exceptions:

- force majeure event
- customer/third-party actions
- scheduled maintenance
- issues caused by customer equipment, data, or technology
Audits

• Three primary types of audit provisions

  • Use audits – audits by the provider of customer’s actual use of the software or cloud services

  • Financial audits – audits by either party of the accuracy of the fees paid in connection with the agreement

  • Security audits – usually in the context of cloud services agreements, audits of provider’s data centers and processes to ensure that provider complies with certain minimum data security standards
Software License Grants

• Licensors of software generally want to make the license grant as narrow as possible to control the usage of the software by the customer

• Customers prefer the broadest license grant possible. Customers want to ensure that the license grant is drafted broadly so that the customer can utilize the software to meet its business needs, and ensure that the license grant permits the customer to provide access to the software to all anticipated users

• If the customer uses contractors/agents, and these contractors/agents need access to the software to provide IT support, for example, the customer should ensure that the license grant is broad enough to permit the customer to provide such access

• Some providers attempt to charge the customer an additional fee if the customer wishes to permit contractors/agents to use the software
Termination/Suspension

• When can a provider can terminate or suspend services?
• Rights may be scattered throughout the document
  • Payment provisions
  • IP provisions
  • Restriction provisions
Terms of Use, Privacy Policy, etc.

• How does a provider’s terms of use or privacy policies impact a customer’s agreement with the provider?

• Does the document undermine the rights and protections that a customer believed it was receiving under its agreement?

• Does the document permit unilateral modification?

• Does the customer have any rights if a modification harms the customer?
Modifications to the Services

• Can the provider modify its services or software?
• What rights do customers have when that occurs?
• Right to modify may be appropriate in some contexts
  • e.g., cloud services
• Essential to understand the parties’ respective rights in this context
  • e.g., the amount of advance notice in connection with those modifications
Some Core Issues in Technology Professional Services Agreements
Professional Services Agreements

Common Errors:

• No way out of agreement
• Elephants in mouse holes (e.g., in boilerplate)
• Often unclear relationships between terms – which controls where there is a conflict (e.g., MSA v. SOW) ?
• Unclear relationships between the documents themselves (e.g., SOWs part of single MSA, or MSA operating as terms incorporated into each SOW)
Statements of Work: Some Key Provisions

• Fee structure (fixed fee vs. time and materials)
• Timing and milestones
• Acceptance of deliverables
• Ownership/rights to deliverables
• Warranties/quality assurance
• Customer responsibilities
• Excuse and suspension of performance
Intellectual Property

- Some issues regarding IP Created in Connection with the Agreement include:
  - Who owns it?
    - Provider?
    - Customer?
  - Provider’s preexisting IP embedded in deliverables
    - What if Customer needs to continue to use deliverable after the agreement ends?
  - Open source software
  - Further acts
Interactive Exercises

Find the Problems with the Provisions
OUR SALT MINE
• Overbroad language

• Unduly narrow language

• Risk exceeds benefits
• **Silence** (e.g., as to timing, who pays the costs, who performs the task, or other material information)

• **Ambiguous language**

• **Loophole words**

• **Toothless RYNOS™** (i.e., rights yet no obligations)
• Misdirection

• Internal inconsistencies

• Non-standard language

• Endless Trouble
Exercise 1: Warranty

1. Provider agrees (a) that each critical component of the software will, under normal use and circumstances, perform substantially in accordance with any materials that Provider may provide to Customer, and (b) Provider will provide support for the software if applicable. If Customer notifies Provider of a breach, Provider will repair, replace or re-perform, as applicable, the nonconforming portion of the software or support, as the case may be.

2. Section 1 does not apply to software that has been (i) repaired, modified, reconfigured, operated, or maintained by any person other than Provider, (ii) used not in conformance with any documentation, or (iii) combined with any third party hardware or software that was not provided by Provider itself. In addition, Provider shall not be deemed to be in breach of this section where the circumstances causing the breach may be beyond Provider’s reasonable control.
Exercise 2: Limitation of Liability

NEITHER PARTY MAY BE LIABLE TO THE OTHER PARTY FOR ANY CONSEQUENTIAL DAMAGES. THE MAXIMUM LIABILITY THAT EITHER PARTY SHALL HAVE TO THE OTHER PARTY THROUGHOUT THE ENTIRE TERM OF THIS AGREEMENT SHALL EQUAL THE AMOUNT THAT PROVIDER HAS RECEIVED FROM CUSTOMER UNDER THIS AGREEMENT DURING THE 3 MONTH PERIOD IMMEDIATELY PRECEDING A CLAIM BROUGHT UNDER THIS AGREEMENT.
Exercise 3: Indemnity

1. Provider will indemnify Customer against any damages incurred in connection with any lawsuit alleging that the Services infringe U.S. patents or trademarks that were in effect before the commencement of this Agreement.

2. Provider cannot be liable for any claim under Section 1 if such claim arises out of or relates to (a) Customer’s use of the Services; (b) any User’s use of the Services not in accordance with the Documentation or Provider’s then-current Terms of Use; or (c) any Customer Data, and in each such event Customer shall indemnify Provider. A party’s obligation to indemnify is contingent upon the other party timely notifying the indemnifying party of any Claim.
Exercise 4: Data Privacy

1. Provider shall take adequate steps to protect Customer Data from unauthorized access by any entity throughout the term of this Agreement, and Provider shall not knowingly share Customer Data with any third-party except in connection with Provider’s exercise of its rights under this Agreement.

2. Provider will perform background checks on all employees who have the potential to access any sensitive Customer Data.
Exercise 5: Security Breach

1. Upon discovery of (a) any unlawful access to any Customer Data stored on Provider’s equipment; (b) any unauthorized access to any equipment; or (c) any incident for which Provider is unable to promptly determine whether any unlawful or unauthorized access to any data stored on any equipment has occurred (each a “Security Incident”), (1) Provider will by the deadlines required under applicable law notify Customer and its users, and (2) the Security Incident shall thereafter be promptly investigated.

2. Provider shall be liable to Customer for any damages as a result of a Security Incident where that incident is caused by Provider’s gross negligence or willful misconduct.