COMMENTARY

What Non-IT Lawyers Need to Know About IT Contracts & Contracting for AI-Related Services

In an age where technology permeates nearly every facet of business, the importance of having a general understanding of Information Technology (IT) contracts is crucial.

November 13, 2023 at 09:15 AM

Contracts

By Evan Foster, Leah Leyendecker & Grace Cheng, Saul Ewing | November 13, 2023 at 09:15 AM

In an age where technology permeates nearly every facet of business, the importance of having a general understanding of Information Technology (IT) contracts is crucial. This article provides a high-level guide for lawyers who don't regularly practice in this area who are tasked with reviewing and negotiating IT contracts, including contracts for Artificial Intelligence (AI) related services.

'Purchase', 'License', or 'Right of Access'

Though a customer may have paid for software, this payment is most likely in exchange for a license rather than a purchase. The software provider retains ownership of the intellectual property (IP) rights in and to the software. Software-as-a-Service (SaaS) agreements are often viewed as service agreements (rather than license agreements) under which the customer obtains remote access to the software services, and not a license under the provider's IP rights in the SaaS services. Thus, providers may refer to the use of SaaS services as a "right of access" or "authorization" rather than a "license."

License Scope

The license grant is the central provision in a license agreement and defines the scope of rights granted, including:

- The licensed product (software, code, data, etc.);
- The term (perpetual, limited period, subscription-based);
- The license rights and permitted uses (enterprise-wide or limited to specific facilities or users);
- Quantity limitations (number of processers, users, employees, etc.); and
- Any additional requirements or limitations.

License Location

In a traditional licensing agreement, software is typically installed on a customer's premises, allowing the customer to configure the software to meet its particular needs in its own environment. With cloud solutions, both the software and the customer's data is hosted by the provider, often in a shared environment with multiple customers on the same server. To minimize security risks, reviewers should understand the provider's data security practices and ensure that contractual language sufficiently protects data.

Product or Service Specification

When contracting for off-the-shelf products, the order form will often simply recite the name of the product. For more complex products, specifications should be included in the agreement to establish a common understanding of the features and capabilities and bind the provider to the functionality promised.

Product Implementation

Many technology products require more than a simple download to implement. An implementation plan, usually in the form of a Statement of Work, should outline the process, timeline, deliverables, milestones, responsibilities, and associated costs of implementation. A milestone-based payment structure helps protect against the risk of provider default or non-performance. Consider whether acceptance testing should be a condition for final payment to ensure that the final product satisfies the agreed upon functionality.

Performance Warranties and Standards

Risk is allocated in part through representations and warranties. Provider representations and warranties should be more extensive than those of the customer. In off-the-shelf agreements, the provider should warrant that the product will perform in accordance with the specifications. Key representations and warranties to consider in negotiated agreements for more complex products include warranties:

- That the provider owns or controls unencumbered rights in the licensed product;
- Against malicious code, including a warranty against ransomware; and
- Regarding interfaces and compatibility.

For SaaS/cloud agreements, warranties are often documented in Service Level Agreements ("SLA") which specify performance standards such as uptime/availability, speed/latency, and response/resolution time for support requests.

Maintenance and Support Services

Maintenance generally refers to periodic updates to correct latent defects and/or improve performance and functionality. Customers should seek an affirmative obligation by the provider to regularly provide maintenance releases. Support services refer to technical support in connection with a specific product. Support

availability varies for off-the-shelf products. For more complex products, support services are often included in a separate SLA, on an exhibit to the agreement, or via a link to a webpage setting out the description of support services.

The agreement should differentiate between license fees and fees for maintenance and/or support. License fees may be paid upfront or on a periodic basis. Beware of concealed maintenance/support fees required to keep the license active. Consider setting a cap on annual maintenance/support fee increases. For longer-term agreements, the provider should guarantee a set duration of maintenance/support and that prior versions of the software will be supported for a period of time.

Data Rights

Ownership rights in data submitted to the provider should be reserved. Seek a broad definition “customer data” to cover all data, information, etc., that is: (a) collected for/from the customer; and (b) any results, output, copies, reproductions, or derivative works of any customer data. Agreements vary in whether and how the customer grants the provider authorization to use customer data, which should be limited to use solely to provide the services under the agreement. Watch for provisions authorizing the provider to mine or aggregate data. If the provider will have possession of any customer data, include a mechanism for getting it back both upon request and termination.

Limitations of Liability

Limitations of liability provisions generally protect the provider over the customer. A provider’s standard form agreement will usually exclude consequential damages and include a cap on the provider’s total monetary liability based on fees paid. If negotiation is possible, seek: (a) mutuality of any limitation of liability provisions; (b) carve-outs from the liability cap for amounts payable as indemnification and liability to third parties arising from the provider’s breach of its obligations concerning ownership, confidentiality, privacy, or security of customer data; and (c) a higher cap on damages—a multiple of fees paid.

Special Considerations for AI-Related Services

In the absence of a comprehensive AI regulatory framework in the US, use of AI products must comply with existing regulations related to privacy, data security, IP, and anti-discrimination, among others. For example, the CFPB is concerned about the discriminatory use of AI in lending decisions and the EEOC is concerned about the use of AI to make employment-related decisions about job applicants and employees.

AI’s increasing influence on critical decisions is inevitable. What is lacking is insight into how these decisions are made. With traditional programmed algorithms, decision making processes are easily understood though their code. With AI there isn’t a way to look into, understand, or verify processes. One way to address this is by translating ethical principles into explicit contractual obligations that are clear, measurable, and enforceable:

- Require the AI service provider to provide transparency reports, conduct regular audits, or implement privacy protection measures.
- If the AI system involves decision-making processes that may impact individuals or groups, specify that the AI service should be designed and tested to minimize biases and avoid discriminatory outcomes.
- Include requirements for regular fairness audits and the mitigation of any identified biases.
- As ethical considerations in AI evolve over time, commit to periodic contract reviews and updates to make sure that the contract remains aligned with emerging ethical standards and practices.

As Saul Ewing's Cybersecurity and Privacy Practice Co-Chair, Evan Foster advises clients on legal issues involving technology, data privacy and cybersecurity.

Leah Leyendecker is an Associate at Saul Ewing who advises clients on a range of corporate and intellectual property matters.

Grace Cheng is a law student at Wake Forest and was a 2023 Summer Associate at Saul Ewing.