ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

IP Risks in Outsourcing: Traps for the Unwary

Intellectual Property

Technology, Privacy, and eCommerce

CHEAT SHEET

- ***Strategize.*** Evaluate your company's risk tolerance and design an intellectual property (IP) strategy that includes vetting and outsourcing agreement protections, like ownership rights, assignments, licenses, and risk-shifting mechanisms.
- ***Identify the IP.*** Protecting patents, trade secrets, and copyrights during outsourcing requires identifying the IP that may be used or created through the engagement and determining how to leverage IP law to meet the customer's business objectives.
- ***Protect the data.*** Data and databases are increasingly being identified as business assets that should be protected through IP rights.
- ***Prepare for the end.*** All outsourcing agreements should address termination and exit rights that guarantee the customer can continue to use IP developed during the engagement after the agreement ends.

Companies are more frequently turning to third-party subject matter experts to outsource their most pressing business needs and critical processes to allow them to cut infrastructure costs, focus on their core competencies, and/or obtain access to new, enhanced technologies. Although these relationships present opportunities for companies to improve product and service quality and leverage economies of scale to better compete within their respective markets, they also pose the risks of exposing potential data and confidential information and mismanagement of technology and

other IP assets. This is because most outsourcing engagements require customers and providers to share a high level of intellectual property, including know-how, which risks theft or misappropriation of trade secrets, diminution or full loss of IP rights, and reduced control of the outsourced function. In addition, whenever parties share data or information, the chances of a data breach and implications related to data security and privacy laws should be a top consideration.

For these reasons, prior to entering any outsourcing engagement, companies should carefully consider the risks and rewards of sharing their technology and IP. A company can reduce its likelihood of exposure by evaluating its own risk tolerance and designing a comprehensive IP strategy that includes due diligence in vetting and managing relationships with potential providers and appropriate protections in the outsourcing agreement. Ultimately, any outsourcing arrangement requires both parties to properly identify their respective data, technologies, and other IP assets and consider how the sharing of such assets can be effectively managed while achieving the overall business objective. This article is a high-level review of IP issues that should be considered in any outsourcing arrangement. For those new to or lightly versed in IP law, consultation with outside counsel is recommended to explore the implications of these principles in the context of a specific outsourcing transaction.

IP rights implicated in outsourcing

The nature of the IP assets involved in an outsourcing transaction will vary depending on the industry, transactional context, and business needs. Where one or more substantive IP rights — patents, trade secrets, and copyrights — may be implicated, protecting these IP rights requires: (1) an identification of the designs, processes, techniques, software, data, know-how, and other technologies that may be used or created throughout the engagement, including any owned or third party-licensed background IP to which the other party may need a license to perform under the agreement and any developed IP, the ownership of which will need to be discussed and likely negotiated by the parties; and (2) a determination as to how best to leverage available IP protections under substantive IP law to meet the customer’s business objectives.

Patents protect new, useful, and nonobvious inventions and vest in the patent owner the right to exclude all others from making, using, offering for sale, selling, or importing the claimed invention. Trade secrets protect information such as formulas, patterns, compilations, programs, or techniques that derive independent economic value from not being generally known or readily ascertainable. Copyrights protect original works of authorship that are fixed in a tangible medium of expression (e.g., a written work or software) and provide owners with a bundle of exclusive rights in their original works for the duration of the copyright.

IP ownership and control

There are several approaches to allocating ownership and addressing use rights of IP that are relevant to any outsourcing engagement. To that end, all outsourcing agreements will include some variation of ownership rights, assignments, licenses, and risk-shifting mechanisms, such as indemnification provisions. Generally, while the provider will want the ability to leverage and profit from the use of IP associated with the engagement across multiple customers, the customer should use its position to maximize ownership and control rights (and, correspondingly, its right to exclude competitors from accessing or benefiting from the IP) during and after the relationship to support business continuity.

Patent outsourcing relationships may involve the creation, use, modification or manufacture of a patentable innovation, and utility and design patents are most common to outsourcing transactions. Utility patents protect the function and operation of patentable innovations, whereas design patents protect the ornamental designs embodied in or applied to articles of manufacture.

In the United States, patents are granted based on a “first-to-file” basis rather than “first-to-invent.” An inventor is defined as the first to conceive and reduce to practice, with conception being characterized as the mental act of having a definite idea of the complete and operative invention such that only ordinary skill would be necessary to reduce it to practice. Since it is possible for a provider to come up with some improvement to a customer’s invention during its delivery of services (particularly with outsourced manufacturing or development services), there is a real potential for a dispute in which the provider could rightfully file first and claim ownership over the invention. It is, therefore, important for customers to anticipate this possibility and contractually define all ownership rights that may result from the engagement, including any foreseeable deviations from the development plans that may occur over the life of the engagement.

Trade secrets

Depending on the characteristics of the new product or process, relying on trade secret protection might be more favorable than filing for patent protection. If the product or process cannot be readily reverse engineered or detected and its secrecy provides some competitive advantage over the market, or the technology moves so rapidly that its competitive advantage is quickly superseded, then it may be better protected as a trade secret. Trade secret protection extends to information that derives economic value because of its status as a secret. Therefore, customers seeking trade secret protection must use reasonable efforts to maintain the secrecy, including confining any dissemination solely to individuals who have a “need to know” and requiring the provider to adhere to contractual confidentiality and restricted use obligations.

Copyrights

Under the US Copyright Act, a work qualifies for copyright protection if it has a minimal amount of creative expression and has been fixed in a tangible medium. Copyright provides its owner with a bundle of exclusive rights, preventing its distribution, reproduction, performance, or exploitation by a third party. In the context of an outsourcing transaction, to ensure that the customer enjoys ownership and control of certain copyrightable works specially ordered or commissioned by the customer and created by the provider (such as drawings, designs, manuals, and other similar materials), the contract should specify that all such works constitute “works made for hire.” In addition, certain other works that do not clearly fall into one of the specific categories of works that qualify as works made for hire (for example software code); so, specifying that the provider is creating a “work made for hire” will not be enough to ensure that the customer owns the work product. Therefore, a customer should also include a present assignment of all of the provider’s right, title, and interest in the work product, including any license rights to third-party content (subject to disclosure requirements and appropriate representations of authority and accuracy), to secure the customer’s rights in the work product.

Data use and safeguards

In today’s data-driven environment, companies are increasingly recognizing the value of data and databases as business assets that should be protected through confidentiality, restricted use

provisions, and possibly one or more categories of IP, including trade secrets, copyrights, and patents. To ensure the maximum level of protection for its data, a company should consider the nature and scope of protection that can be secured under the various types of IP rights; and implement policies and procedures for maintaining the security and confidentiality of the data. The company should also incorporate into the outsourcing agreement adequate safeguards against unauthorized use or disclosure, return of the customer's data at the end of the relationship, and support to transition to an alternate provider or back in-house.

In recent years, a trend has arisen with providers including "aggregated data" provisions in certain types of outsourcing contracts that allow them to compile, collect, and use the customer's data on an anonymized, de-identified basis for their own business purposes. Particularly in software and other technology agreements, providers seek to leverage big data to run their own analytics on the relevant market, as well as enhance their own services. A customer's initial reaction might be to strike this provision based on data privacy concerns, however, the common landing place is that the customer will accept the overall concept but include appropriate limitations and clarifications on the provider's use of the data derived from the customer's data.

> In recent years, a trend has arisen with providers including "aggregated data" provisions in certain types of outsourcing contracts that allow them to compile, collect, and use the customer's data on an anonymized, deidentified basis for their own business purposes.

The customer's right to disclose and permit the specified data aggregation and use by the provider is a threshold requirement. If this condition is satisfied, it is important that aggregated data provisions specifically state the data points the provider may aggregate, the manner by which it will be anonymized and de-identified, how it will be aggregated with any other data, and the specific business purposes for and manner in which the aggregated data may be used. Above all, the customer should make certain that the provider takes the necessary steps to ensure a third party cannot deduce that the customer was the source of the aggregated data from the data points captured. As trends in transformative technologies (such as artificial intelligence (AI) and the Internet of Things) continue to place a higher value on big data, aggregated data provisions in outsourcing agreements present an opportunity for customers to make a concession that can support hardline stances elsewhere in the contract.

Specific transaction contracts and IP concerns

While the nature of IP involved in any outsourcing deal varies depending on the transaction, there is still a general framework that can be used to approach IP concerns in any engagement. In all cases, this begins with an inventory and assessment of relevant existing and future IP, including all requirements necessary to effect and perfect the assignments, transfers, and licenses the customer needs to achieve its operational objectives.

The IP assets contributed to or created in any outsourcing transaction fall somewhere on a spectrum based on the goods or services procured. On one hand, outsourcing a particular business process or a contract manufacturing deal creates a dedicated service model specifically tailored to the business. In these transactions, the customer will require greater control over the relevant IP used and created and the corresponding ownership rights, extending limited rights to the provider, which may be exclusive to the customer or otherwise restricted to noncompetitive uses. On the other end are solutions where the provider employs a shared delivery model (for example, software-as-a-service solutions). The nature of these services is such that providers often use a multi-tenant (or "one to

many") environment to provide the services in order to provide scalability. In these types of transactions, the services are less customizable, and the customer typically has less control over the services and, correspondingly, the ownership of the IP underlying the solution. Somewhere in the middle exist varying types of software and IT engagements whose scope depends on the extent of services and, therefore, alters the bargaining powers of the provider and customer when the control and IP ownership are shared between the parties. Regardless of where a particular outsourcing transaction falls on this spectrum, further investigation into the IP considerations inherent in different contexts reveals that while nearly all are implicated in every engagement, some require more protections and attention than others.

Product development and contract manufacturing includes everything from the design and production of a small component to the creation and supply of entire products. In most cases, the customer owns or expects to own the IP in the product designs and workflows, although the customer may need licenses to the manufacturer's background IP (both during the term and after) to the extent embedded in or used to produce the manufactured products.

In product development and supply outsourcing, the critical message is that payment for deliverables does not by itself transfer ownership or other rights in the work product of the service: rather, a clear and present written assignment is required to secure ownership of IP. Because development may continue into the production phase with product modification or customization, customers must be diligent in exercising upfront leverage to lock in all IP ownership, control, and license rights necessary to ensure a competitive market position and supply continuity.

The tangible nature of contract manufacturing makes patents to those physical products and processes the most obvious IP asset. Prior to making any disclosures to a provider, customers should consider certain statutory bars that may prevent the customer from obtaining patent protection. For example, the on-sale bar prevents an inventor from obtaining a patent if the invention was publicly disclosed or on sale for more than one year prior to the filing date of the patent application. Therefore, to protect an invention, companies must either file for patent protection within one year of the first public disclosure or, preferably, before engaging the provider. It is worth noting that the processes involved in a contract manufacturing engagement might also be protectable by trade secret.

If the product being manufactured requires provider access to sensitive trade secrets and know-how of the customer, a company might consider taking extra precautions in protecting its patentable inventions and trade secrets, such as (1) working with multiple providers on different phases so that no one manufacturer has access to all of the procedural details and (2) specifying in the contract that the provider must follow any listed steps exactly as written and that the finished product must meet the exact specifications to ensure that the provider cannot retroactively claim that it added a sufficiently new element to the process that warrants a claim for inventorship.

The customer should also consider IP related to the manufacturing process, equipment, or tools. The contract should protect and limit the use of process know-how, tools, or other tangible or intangible assets provided by the customer to the provider to support manufacture or supply. Where the provider controls the manufacturing process, the customer may want to consider negotiating upfront a license grant and obligation to transfer know-how and provide transition support in the event that supply is interrupted or transferred for any reason.

Business process outsourcing (BPO) involves the outsourcing of financial or other "back office" business processes (e.g., accounting, call centers, retail, and human resources) to third-party

providers. Companies often opt to outsource certain business processes because it affords them greater operational flexibility, access to innovative technologies and practices, and improved productivity and efficiencies.

BPO transactions often involve the assignment of a customer's rights and obligations under third-party contracts to the provider. Alternatively, the customer can appoint the provider as its agent for purposes of managing the contract on the customer's behalf. Either way, the parties must determine whether the counterparty to the contract is entitled to withhold consent. If consent is required, the outsourcing agreement should address each party's responsibility for obtaining the consent and how a failure to obtain consent will impact service scope, fees, and other terms of the arrangement. If the provider manages the third-party contract on the customer's behalf, the outsourcing agreement should address the process for designating the provider as the customer's agent, and provide a clear description of the scope of the agency, as well as covenants requiring the provider to comply with the terms and conditions of the third-party contract and indemnify the customer against liability arising from a claim of breach.

Customers also should carefully consider the scope of licenses given by the provider, including: (1) the duration of the license and any right of the provider to revoke the license; (2) whether the license is exclusive or nonexclusive; (3) whether the license is transferable or sub-licensable; and (4) the restrictions on permitted purposes and/or authorized users. The license should specify which party owns any permitted modifications to or works derived from licensed IP. Continued use of provider IP after termination may be critical to in-sourcing or re-sourcing the services without disruption; if so, the license grant should include post-termination rights and transition support. The customer may grant licenses to allow the provider to use customer or third-party IP solely for the purpose of performing the services. If know-how or trade secrets are licensed, appropriate confidentiality and security obligations must be included in the agreement to ensure that the owner's rights are protected. Customers also may use the work for hire doctrine under federal copyright law and a present assignment of rights in arising IP to ensure that copyright in developed works vests in the customer.

Software development and maintenance are characterized by ongoing cycles of design, build, bug fixes, updates, and upgrades designed to comply with evolving market demands. Because it is costly for any enterprise to maintain teams that can meet all these needs for every piece of desktop and application software in an organization, outsourcing is common.

Customized software development may implicate IP protections in the form of patents, copyrights, or trade secrets. Since the Supreme Court's decision in Alice, it has become more difficult (but not impossible) to obtain patents on software or computer-implemented inventions in the United States. Companies seeking copyright protection for source code in the United States must accept that at least some portion of the source code will have to be published and made available to the public during the application process. Many companies opt not to pursue copyright registrations and instead rely on trade secrets to protect their source code and information. In any event, any outsourcing agreement for software development must contain a clear and present assignment of arising IP, appropriate licenses to pre-existing code that may be included in or with the developed software, and strong warranties and representations (backed by equally strong indemnities) of the provider's authority to make these grants.

> Since the Supreme Court's decision in Alice, it has become more difficult (but not impossible) to obtain patents on software or computer-implemented inventions in the United States.

In recent years, publicly available source code known as “open source” has become widely used in all areas of software development. Providers often leverage open source software as building blocks to their developed solutions as a cost-effective way to develop and distribute software. However, some open source licenses contain “copyleft” provisions, which are designed to ensure that the code remains freely available by requiring the source code and any derivatives or modifications to be made available for use and distribution on the same terms. As a result, in any software development transaction, customers should evaluate implications of “copyleft” licensed open source based on their intended use or distribution of the developed software, including whether a contractual prohibition or restriction on use of “copyleft” licensed open source is necessary to protect customer-provided code. In addition, with open source software there is no certainty as to the original source of the code or the developer’s rights, if any, to the contributed code. Because the IP rights to the programs cannot be verified, and generally are made available on an “as-is” basis, a customer allowing use of such a program risks: (1) infringement claims arising from its own use and (2) indemnification claims asserted by end users and licensees of the software or relevant technology if the customer is planning to redistribute the software developed by the provider. To mitigate these risks and in addition to limitations on the incorporation of “copyleft” licensed open source in deliverables, the customer could also include remedies such as replacement of infringing code with a non-infringing open source or commercial alternative, or (assuming the software is not business-critical or is easily replaceable) a refund of the fees paid by the customer.

Cloud services solutions offer varying stacks of infrastructure, operating systems, and software in one package offered by the provider and accessible to the customer over the internet in order to provide flexible solutions. There are three main types of cloud services: (1) Infrastructure-as-a-Service (IaaS), which provides computing resources, servers, storage, and network capabilities on which the customer can run its operating systems and software; (2) Platformas-a-Service (PaaS), which provides customers with access to a development platform and the ability to deploy and manage its software applications through the cloud; and (3) Software-as-a-Service (SaaS) through which providers host, manage, and support the software applications that are accessed by their customers via the internet. Generally speaking, all three of these can take the form of a “one-to-many” delivery method such that the provider hosts the same or similar versions of the product for multiple customers. For that reason, customers may have limited negotiating power over any of the IP in the underlying solution provided by the provider. Instead, data control and access rights are key to any cloud outsourcing transaction. The cloud services contract should contain detailed provisions acknowledging customer ownership and control of its data, including where the data is stored and transmitted, who may have access to it, the extent to which it is encrypted, whether the provider has any right to access or audit it, and what happens to the data upon expiration or termination of the cloud services agreement. It is also important to ensure that the definition of “customer data” includes all aspects of the data that the customer expects to own, including input and derived data. Last, the customer will want to ensure that it has access to all its data in a commercially reasonable format both during the relationship and for any transition period of time after the relationship ends.

Artificial intelligence (AI), a transformative technology, presents some unique challenges and considerations to IP rights. AI is being used across nearly every industry and is further developing into a more adept decision-making tool thanks to advancements in neural networks and machine learning. AI is proving capable of not only changing business processes but also how we view IP ownership in the digital age. Identifying the author of a work, inventor of a new process, or owner of a data set was previously straightforward, but that changes once an AI algorithm generates the work product. Unlike in the traditional software development context, machine learning can automatically generate and derive software code without human intervention, therefore, creating disputes relating to who owns the IP rights in the code. Specifically, under current law copyrights only arise for works

produced by a human being (similarly, the US Patent Office requires a patent application to be filed in the name of a human inventor). Because an AI system is not (yet) considered a legal person, there is not yet a standard to decide when the human element of coding gives way to an AI-driven decision. Still, companies working with AI outsourcing providers should consider whether it is appropriate to include provisions in the contract that any new works, innovations, or processes later created by the AI system are assigned to the company, in case these issues are ultimately decided in favor of copyright.

Exit rights / termination

No matter the type of outsourcing transaction involved, the outsourcing agreement should address exit from the relationship in a comprehensive manner. At a high level, this means that the customer should consider how long it will take to transition to a new provider and what it will need from the incumbent provider to accomplish a smooth transition. From an IP perspective, it is important to ensure that the customer's right to access and use IP created in the course of the engagement extends beyond the term of the outsourcing transaction.

References

35 U.S.C. § 154(a).

17 U.S.C. § 106.

17 U.S.C. §201(b).

Alice Corporation Pty. Ltd. v. CLS Bank International, et al., 134 S.Ct. 2347, 2353 (2014) (holding patent-ineligible computer software for an intermediated settlement system).

ACC EXTRAS ON… Protecting IP

ACC Docket

Best Practices to Protect Trade Secrets in Failed Acquisitions and Customer Relationships (Nov. 2019).

Vanishing IP: 6 Tips to Secure Your Company's Most Valuable Assets from Departing Employees (April 2018).

Sample Forms, Policies, and Contracts

Key Metrics for Intellectual Property Portfolio Measurement (Oct. 2018).

Sarah Beisheim

Legal Counsel

REMADE Institute

Sarah Beisheim is legal counsel for REMADE Institute, a Manufacturing USA® Institute and division of Sustainable Manufacturing Innovation Alliance Corp. She previously spent more than 24 years with Xerox Corporation, where she was senior IP counsel and lead product counsel focusing on complex commercial and intellectual property transactions.

William Eipert

Senior Counsel and Lead Advanced Development Counsel

Xerox Corporation

William Eipert is senior counsel and lead advanced development counsel for Xerox Corporation counseling Xerox’s research and product development organizations across a range of strategic intellectual property and commercial transactions including acquisitions, divestitures, outsourcing, licensing, joint development, sponsored research, and OEM arrangements.

Josh Ganz

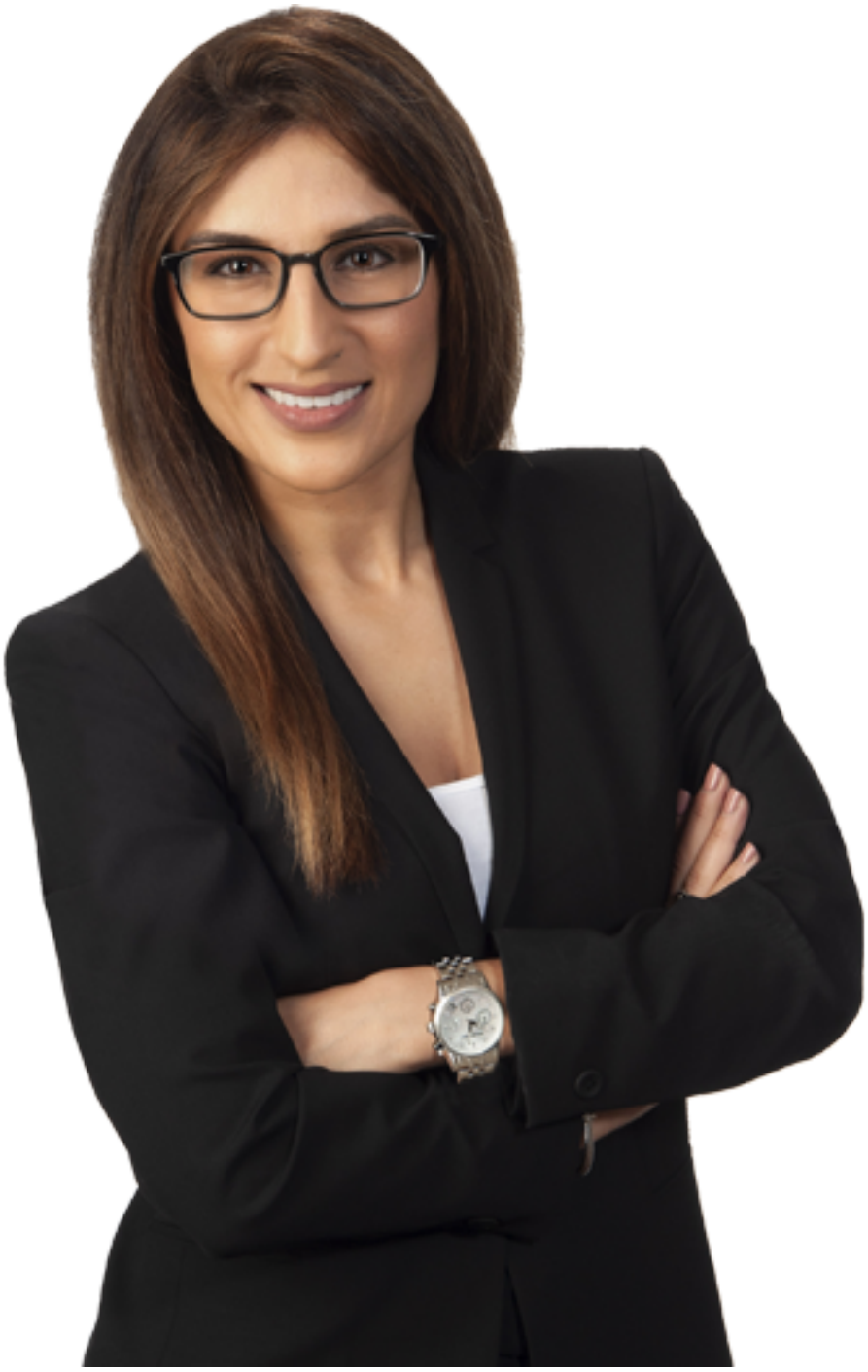
Partner

Atlanta office of Kilpatrick Townsend

Josh Ganz is a partner in the Atlanta office of Kilpatrick Townsend. He focuses his practice on strategic outsourcing, technology licensing and procurement, strategic alliances, joint ventures, and

other complex transactions.

Maha Khalaj



Associate

Atlanta office of Kilpatrick Townsend

Maha Khalaj is an associate in the Atlanta office of Kilpatrick Townsend. She focuses her practice on technology and intellectual property licensing and procurement, outsourcing, and other complex commercial transactions