Ketan Pastakia is counsel in the Technology Transactions Group within the Firm's Merger & Acquisition Practice.
Ketan concentrates his practice on transactions involving the development, acquisition, transfer, and licensing of intellectual property and technology. He represents multinational corporations in a variety of industries, including Internet software, mobile devices, autonomous vehicles, drones, semiconductor technology, hardware manufacturing, and medical services. Ketan has significant experience with joint ventures, joint development and strategic alliances, distribution and supply agreements, hardware/software licensing, open source issues, cloud computing and data privacy protection.

Ketan has also represented clients in complex patent litigation matters and has experience with pre-suit investigations, document discovery, invalidity and non-infringement contentions, inter partes reviews, expert reports and depositions.

Ketan holds a bachelor's degree in electrical engineering and a master's degree in information networking. Prior to attending law school, he spent many years as a senior technical analyst and project manager for telecommunications companies.

Genevieve Dorment is a partner in Willkie's Intellectual Property Department. She has extensive experience advising companies, private equity firms and exempt organizations in all intellectual property, privacy and technology aspects of corporate transactions, including mergers and acquisitions, capital markets and financing transactions, licensing, strategic agreements and U.S. trademark applications and registrations. She also advises on intellectual property enforcement matters.

Genevieve has represented leading private equity firms including Centerbridge, Calera Capital, Corsair Capital, EQT, First Reserve, Hellman & Friedman, KKR, KSL Capital, New Mountain Capital, Silver Lake, Stonepeak, Stone Point Capital, True Wind and Warburg Pincus on numerous transactions. She has also counseled exempt organizations, including Carnegie Corporation of New York, Doctors Without Borders, Gray Foundation, Natural Resources Defense Council and Wellspring Philanthropic Foundation, among others.

Genevieve has given lectures for the New York City Bar Association and the American Law Institute. She is also a group leader in Leading Women in Technology's WILpower leadership program.

MARSH

Professional Biography

Laurie Forkas

Senior Assistant General Counsel

Current Responsibilities

Laurie is Senior Assistant General Counsel for Marsh & McLennan Companies, Inc. (MMC) and is based in MMC's New York office. She has worked for MMC for close to nineteen years and has held various roles in MMC's Legal Department. Laurie is currently the Corporate Counsel for Marsh Captive Solutions globally and provides advice on a broad range of legal and commercial issues. In addition, she is Corporate Counsel for Marsh's US Brokerage Operation. In this role, Laurie provides legal advice to her US colleagues and negotiates a variety of contracts, including: Technology Agreements, SaaS, Master Service Agreements, Broker Agreements and Data Privacy/IT Security Agreements.

Experience

Qualified in Ohio, New York and London, prior to joining MMC, Laurie was a technology lawyer for a boutique law firm in New York City - Hall, Dickler, Kent, Goldstein & Wood, LLP. Earlier in her career, she lived in London working for Trans World International, Inc. as In-House Counsel and also lived in Vienna, Austria where she supported executives developing international opportunities.

Her first career position was Senior Law Clerk in the Eighth District Court of Appeals, in Cuyahoga County, Ohio.

Education

- JD, Cleveland Marshall College of Law, Cleveland, Ohio
- BA, Catholic University of America, Washington, D.C.

Boards

New Rochelle Fund for Education Excellence, Board Member since 2021

Daniel advises clients in the Fintech, blockchain, defi, Web3 and NFT ecosystems – and those who interact with them – on the strategic and commercial issues core to their business models, particularly at the intersection of intellectual property and data. He serves as global head of Orrick's multi-disciplinary Fintech practice.

Daniel works with a variety of innovative tech companies at all stages that are adapting to the fast-changing tech and regulatory ecosystem by helping them develop practical, risk-adjusted solutions, including:

- Personal data collection, processing, sharing and commercialization strategies and transactions;
- Intellectual property and personal data concerns involved in the development, deployment and analytics of public and private blockchains;
- Cryptocurrency ecosystem development, foundation formation and operations;
- Cryptocurrency API, analytics, custody, staking and liquidity collaborations;
- Data licensing in the Fintech, adtech and cryptocurrency ecosystems;
- NFT strategy and program development for brands, talent, agencies, minters and marketplaces;
- Development, licensing and software-as-a-service, hosting-as-a-service and platform-as-a-service arrangements for emerging and leading technology companies;
- Patent acquisition and cross-licensing arrangements in the financial and semi-conductor industries;
- Synthetic joint ventures, mergers and acquisitions and capital market transactions across an array of industries; and
- Intellectual property and personal data drop-down financings in the mobility space.

Daniel has been recognized by *Legal 500* 2022 as a 'Next Generation Partner' for Technology Transactions. He has written extensively on cryptocurrency ecosystem matters, privacy and personal data structuring and compliance issues. He serves as adjunct professor at Cornell Tech, where he teaches a course on Fintech and Crypto start-up issues. Before becoming a lawyer, Daniel spent several years teaching physics in Doha, Qatar.

WFG®

CLE

Negotiating Commercial Agreements

Genevieve Dorment, Partner, Willkie Farr & Gallagher LLP
Laurie Forkas, Senior Assistant General Counsel, Marsh & McLennan Companies
Daniel Forester, Partner, Orrick Herrington & Sutcliffe LLP

Overview

- Hot Topics
  - Arbitration Issues Trending in Courts
  - Conditional IP Licensing to Mitigate Supply Chain Risk
- Avoiding Common Pitfalls
  - IP Ownership
  - Acceptance
  - Service Level Agreements
  - Warranties
  - Indemnity
  - Limitation of Liability
  - Confidentiality
  - Source Code Escrow
  - Assignment
  - Fees and Payment
  - Audits
  - Publicity
  - Non-Solicitation

Arbitration Issues Trending in Courts

- Arbitration clauses are not to be overlooked as they have become strictly applied in litigation matters.
- Courts are trending towards construing and enforcing arbitration clauses based on their plain language.
- The Supreme Court has lowered the threshold for arbitration waivers in *Morgan v. Sundance*, 142 S. Ct. 1708 (2022).
  - The Federal Arbitration Act (FAA) entitles a defendant to file an application to stay pending litigation if parties originally agreed to arbitrate.
  - In *Morgan*, the Court held that the FAA did not grant federal courts authority to require a finding of harm before a party could waive arbitration rights.
  - Specifically, the Court reversed the 8th Cir. in requiring a party to show prejudice for waiver to be granted.
  - The Court ruled that federal courts may not create new procedural rules based on the FAA's "policy favoring arbitration."
- The practical takeaway: parties seeking arbitration will need to be very clear in drafting and parties opposing arbitration may have more avenues to litigate based on the exact terms used in the agreement.

Conditional IP Licensing to Mitigate Supply Chain Risk

- Supply chain disruptions are a common risk that buyers face.
- Buyers can mitigate supply chain risk by negotiating for conditional licenses to patents and other IP assets.
- A conditional license would allow buyers to use the seller's IP to source the delayed component/product/service in house or from a third party.
  - However, buyers should be prepared to pay an additional fee to use the conditional license.
- The terms should specify:
  - The scope of the conditional license.
  - The events that trigger the conditional license.
    - E.g., for convenience, failure to meet volume requirements, failure to meet demand requirements, delay beyond target delivery date.
  - The duration of the conditional license.
  - The costs associated with using the conditional license (e.g., royalty fee).

Avoiding Common Pitfalls

IP Ownership

- If development aspect included:
  - Parties generally own their background IP and improvements thereto and negotiate ownership of newly developed materials.
  - Vendor will want to own developments planned to be used in production.
  - Ensure there is full and sufficient language to transfer ownership of any deliverables, including presently assigning IP, deeming copyrightable works to be works made for hire and including further assurances language.
- Even if no development aspect, there may still be:
  - Feedback on the software. Feedback is usually owned by or broadly licensed to the vendor. Make sure the client is aware of this.
  - Improvements, output or other derivative works. Ownership of these items should be clearly delineated and the customer should, at a minimum, have broad license rights to output.
- License scope:
  - What does licensee plan to do with the software? Who else needs to use it?
    - E.g.: access, use, reproduce, copy, design, develop, modify, create derivative works of, implement, make, have made, assemble, test, market, offer to sell, sell, re-sell, disclose, display, perform, transmit, distribute, import, commercialize, support, repair, exploit, dispose of…and have others exercise such rights on behalf of licensee.

Acceptance

- Deliverables and services should often be subject to acceptance.
  - Licensee may want to inspect and test all materials received upon delivery.
  - Acceptance is generally subject to the materials and services meeting acceptance criteria defined in the agreement:
    - Materials should fully conform and be in full compliance with the applicable functional requirements, specifications, any other requirements and/or criteria, and any other quality standards with respect to such materials.
    - They should be free from errors and defects (and from physical damage if applicable).
    - They should otherwise comply with all terms and conditions of the agreement (including the warranties).
  - Failure to meet acceptance criteria generally allows for rejection and the remedies specified in the agreement. Parties may agree to:
    - Afford one or more extensions of time to correct the non-conformities at no additional cost to the customer.
    - Accept the defective materials or services for a reduced price to be negotiated.
    - Terminate any pending materials or services (sometimes with additional penalty and/or full refund).

Service Level Agreements ("SLAs")

- Critical to SaaS agreements as availability of the service is key.
- Sets standards for performance:
  - Uptime commitment (e.g., 99.99% other than scheduled maintenance, force majeure events, network issues and customer-caused downtime).
  - Response time (usually based on priority of reported issue).
  - Resolution time (also usually based on priority of reported issue).
- Usually also sets remedies for breach:
  - Service credits, which are usually a percentage of the monthly fees, which varies based on how bad the service level miss is or how many misses occur.
  - Vendors will resist providing refunds, but a refund should at least be paid if a credit is accrued in the last month of the term.
  - Termination rights can usually kick in if service level breaches exceed X in a calendar year or occur for X consecutive months.
- If client will be selling any products or services dependent on the licensed product, it is critical to make sure client's own SLAs to its end customers line up with the vendor's SLAs and that the vendor's SLAs to client are as good or better so that there is no gap.

Warranties

- Basic Warranties
  - Operation of software/services conforms with documentation.
    - Provide a set time period (typically ranging from 30 days to entire term).
    - Oftentimes vendors push for re-performance or fixing the issue as the sole remedy. If service is not critical, this is usually ok if re-performance / fix is of no cost and customer can terminate and receive a refund if re-performance or the fix is insufficient or not timely.
  - Services will be provided in a professional and timely manner.
    - Vendors often propose services be performed in a workmanlike manner, but this is a lower standard than "professional."
    - Reject re-performance as the sole remedy. Re-performance for a breach in professionalism is a remedy that does not address the injury. E.g., if a vendor employee harasses someone, how does re-performance address that?
  - Compliance with all relevant laws.
    - Privacy law compliance particularly material.
      - Take proactive measures to ensure protection of user and employee data.
    - If a website is being created, then there must be warranties that the website is ADA-compliant.
- Other Warranties to Consider:
  - Ensure there are no viruses.
  - Include a clause that there will not be copyleft open source
  - Consider ethical warranties, such as no use of slave/child labor/fair employment practices/equal opportunity workplace or other priorities for your client (such as diversity initiatives or environmental standards).
  - Include non-infringement/ownership of materials language.
    - Consider addressing effects of IP ownership/validity challenges.

Indemnity

- Scope
  - Subject matter of indemnity.
    - Third-party infringement is the most common, and often most important, type of indemnity.
    - Try to always include gross negligence, willful misconduct, fraud, and violations of law.
    - Add language regarding third party claims caused by breach.
  - Make sure to be specific as to what the indemnity covers. Address:
    - Infringements of what types of IP are included in the indemnity.
    - Are all categories of damages included in the indemnity or just finally awarded judgments and/or settlements?
- Exceptions – indemnifications will often exclude the following:
  - Combinations of products and products/materials not furnished by parties.
  - Unauthorized repair or use of products – including modifications or improvements.
  - Customer-provided specifications. This type of exclusion is often too broad. Try to pare back, knowledge-qualify or remove altogether.

Indemnity - Cont’d

- Procedure
  - Mitigation
    - Any replacements or modifications to mitigate infringement should be of the same or better quality as the original parts.
    - If vendor is allowed to terminate, customer should receive at least a pro rata refund of fees.
  - Notice of Claim – Delay in providing notice of indemnity should not excuse indemnification except to the extent the indemnifying party is materially prejudiced by the delay.
  - Assistance with Claim – Indemnified party should be reimbursed for assisting the indemnifying party.
  - Control/Settlement of Claim – Indemnified party consent should be required for settlement if rights may be adversely affected or if it would be required to admit fault.
  - Insurance – Whether to require insurance be held by the vendor depends on counterparty. More important to require insurance for start-ups.
    - Types of coverage expected include general commercial liability insurance, cyber liability insurance, E&O insurance and statutory required workers’ comp insurance.

Limitation of Liability

- Limitations of liability will include a cap on damages and waiver of indirect/consequential damages.
- Limitations of liability should always mutually apply.
- Cap Amount
  - The higher, the better.
  - Include details on how the cap will apply (e.g., is it an aggregate cap for all claims, limited to a specific period of time such as an annual cap?).
- Exceptions/Carve-Outs – the agreement should specify whether these exceptions open parties up to unlimited exposure or if the different categories follow different cap structures.
  - Indemnification obligations, including intellectual property claims, are usually uncapped.
  - Confidentiality and/or data breaches are usually subject to a super-cap.
  - Warranties or breach of compliance with certain laws are often capped, but not always.
  - Gross negligence, fraud or intentional misconduct are usually uncapped.
  - Payment obligations and infringement of IP are vendor-friendly carve-outs.

Confidentiality

- Consider scope of confidential information in play.
  - Make sure all of client’s sensitive information is covered by definition.
  - Data privacy and security may come into play.
    - Is data being processed by the vendor?
      - If yes, add in data privacy protections.
    - Any PII? If so, is any of it from Europe or European citizens?
      - If yes, add GDPR addendum.
- Residuals
  - Residuals clauses allow the vendor to own know-how it learns performing services. These should be removed or significantly limited, especially if the vendor will have access to sensitive materials.
- Be sure to include an injunctive relief clause for breaches of the confidentiality clause and an obligation to return or destroy any confidential information at the end of the term.

Source Code Escrow

- Is a source code escrow necessary?
  - Does client incorporate the licensed materials into anything it re-sells to its own customers?
  - Does client rely on vendor for upkeep and/or updates to the licensed materials?
  - How easily could a second-source step in and take vendor's place?
- Typical trigger events for escrow:
  - Bankruptcy (voluntary or involuntary) or insolvency (financial tests).
  - Vendor ceasing operation or dissolution of vendor's business or a substantial portion thereof or dissolution or transfer of substantial portion of the assets which are the subject matter of the agreement.
  - Change of control to any party who does not agree to fully perform under agreement.
  - Material breach of the agreement, although this is a much less common trigger event.
- Client will likely want to pay for verification services.
  - Use/function verification.
  - Independent build verification.
- Do not allow the vendor the ability to stop escrow agent from releasing upon trigger event.

Assignment

- Generally should push for restrictions on assignment to be mutual.
  - In certain cases where the know-how of the vendor is critical, there should be no assignments by the vendor without customer consent.
  - Exceptions to assignment:
    - Affiliates, but assignor should remain liable unless assignee is an entity of similar creditworthiness, otherwise there is a risk of assignment to a shell.
    - Changes of control (asset sales, mergers, stock purchases).
- Divested entity rights
  - Divested entity rights allow a customer to provide divested entities services via TSA.
  - Divested entity should be able to use the services/software for its own business or in service of the customer's business.
  - Divested entity rights period is usually between 6-24 months.
  - May not be applicable depending on the service/software.
  - If client is frequently divesting entities, then fees should be adjusted following divestment.

Fees and Payment

- Due dates for payment
  - The longer a due date, the better.
  - Market is between 30-60 days, with 45 days being the usual compromise.
  - Customer should be able to withhold fees disputed in good faith.
- If client will be making payments up front, be sure to include refund terms in the event of early termination.
- Late payments
  - Interest for late payments is market, but the rate should be as low as possible.
  - Sometimes vendors also push to recover collection costs, which should be rejected.

Audits

- An audit rights clause builds certainty and trust between the parties.
- The right to audit the other party is typically mutual.
    - Can extend to financial and non-financial matters.
        - E.g., costs, payments, warranties, covenants, compliance.
- Consider the scope of the audit rights and who should bear the cost of an audit when negotiating.
- Vendor will prefer broad audit rights for things like customer’s compliance, including seat license compliance, but will want more limited rights for verifying fees or verifying vendor’s compliance.
- Customer will prefer to limit audit rights for its own compliance, but will want broader rights for vendor’s compliance and for verifying that fees are calculated correctly.
    - Purpose of audit and scope of access should be specifically described.
- Limitations on audit rights often include:
    - Limiting audits to once per year (unless there is a prior discovered breach).
    - Requiring reasonable advance notice of an audit.
    - Conducting the audit in a minimally disruptive manner during normal business hours.
- It is crucial that auditors be subject to confidentiality restrictions as restrictive as those set forth in the agreement.
- Often the auditing party pays for the audit, unless there is a material discrepancy, in which case the fees often shift.

Publicity

- General rule of thumb should be to prohibit use of customer name or identification of customer as a client of the vendor without the customer's prior consent.
    - Any exceptions should be explicitly pre-agreed.
- Similarly, place limits on announcement of the deal or listing client as a partner or customer.
- If client's name will be used, make sure to include trademark controls, such as:
    - Sample approval.
    - Termination rights.
    - General quality control.
    - Covenants not to challenge client's trademarks.

Non-Solicitation

- Should favor client or at least be mutual.
- Should be time-limited for practicality purposes.
- Should only apply to employees and not to contractors.
  - Should only apply to employees who had contact with the other party over the course of the services.
- Carve out ability to advertise positions generally and to respond to unsolicited inquiries and applications.
- Carve out ability for employees to unilaterally approach potential employer.
- Carve out employees who are terminated.
- Be aware of relevant state laws (e.g., California) even if the governing law of the contract is for a different state.
- Be careful of antitrust: non-solicitation agreements have become a focus in antitrust litigation as certain practices may have anti-competitive effects.