2025 NYIPLA TRANSACTIONS BOOTCAMP

DAY 3 – M&A DUE DILIGENCE

Jonathan Berschadsky
Merchant & Gould PC

Christopher Loh,
Venable LLP

Timothy McNamara
Goldman Sachs

Briana Barron
Arcus Biosciences

DISCLAIMER

The opinions herein are those solely of the speakers,
and do not reflect those of the speakers' organizations or clients.

TODAY'S AGENDA

- Diligence Basics

- Data Room

- Non-Data Room Diligence

- Substantive IP Analysis

- Reviewing Deal Documents

- Ethics

DILIGENCE BASICS – Types of M&A

Types of IP M&A:

- Horizontal, vertical, concentric, market-extension or product extension, conglomeration, stock purchase, asset purchase, collaboration.

Key Focus:

- Avoid getting bogged down in corporate transaction details.

- Prioritize IP transfers and the underlying technology/science to ensure that the assets critical to the deal align with your business goals.

- Understanding the specific IP being transferred helps identify potential risks, such as licensing restrictions, pending litigation, or enforcement issues.

- This focus will guide document review and the key questions to ask during discussions (e.g., conference calls with key personnel).

DILIGENCE BASICS – Key Purposes

➢ Purpose of M&A: to acquire rights to a patent portfolio that, in the worst case, can be asserted or defended in litigation

 ❑ Documents sufficient to ensure acquiror has standing to sue
 ❑ Documents that may indicate warts (validity/enforceability concerns)

➢ Purpose of M&A: collaboration
 ❑ Third party inbound/outbound-licenses

DILIGENCE = AN INSURANCE POLICY

- Determining the Appropriate **Scope and Focus** of Diligence
  - Tailor diligence based on client goals, risk tolerance, and priorities

- **Minimizing Risk**: How much risk (time and $$) is client willing to take on?
  - Identify client's goals
  - Which IP or products/services matter?
  - Who are competitors?

- Identify issues important to business objectives
  - Patent protection / Barrier to entry / Term of exclusivity
  - Freedom to operate / Litigation concerns
  - Company-Owned IP / In-Licensed IP
  - Trade Secrets / Key employees

TYPES OF IP TRANSFERS

- M&As typically involve the following types of IP transfers:

  - Full acquisition of target company and all its IP assets

  - Partial acquisition of certain business of target company and related IP assets

  - Collaboration agreements, in which IP is split or jointly owned

  - License agreements

  - Discovery agreements

- Many M&As involve multiple types of IP transfers. For example, a partial acquisition may require a license-back by the acquiror to the target of IP that overlaps both the acquired business and the target's retained business.

7

DILIGENCE BASICS

- Most deals involve several different types of lawyers.

- Only a small cohort of those lawyers have relevant experience with intellectual property or underlying technology/science.

- As IP counsel, you will be uniquely suited to spot and advise on:

    - IP-related legal issues

    - Technology/science related issues

- It is your job spot and **to propose solutions** to those issues.

DILIGENCE BASICS – TIMING

- The timeline for conducting diligence will be dictated by factors beyond your control, including:

  - Business/regulatory issues

  - Data room opening

  - Data room population

  - Public announcement of deal

  - Closing date

- Many due diligence tasks will be of the "hurry up and wait" kind!

- Be flexible and patient.

DILIGENCE BASICS – CLIENT INTERACTIONS

- Ideally, **a single line of communication** should flow between the deal lawyers at your firm and the in-house lawyers at the client.

| Junior associates | Senior associates/counsel/partners | Lead partner | Client |

- Without a single line of communication, key issues may be miscommunicated or missed, and confidentiality may be put at risk.

- There are exceptions: check with more senior members of the team before communicating directly with client/outside-counsel.

DILIGENCE BASICS – CLIENT INTERACTIONS

- Beware of **memorializing negative issues in writing** without prior client approval.

  - Such written communications may unnecessarily expose the client to liability.

- Ideally, a negative issue should be discussed first with the client on a call.

- If the client asks for a written communication addressing the issue, use appropriate measures to preserve attorney-client privilege.

- Do not identify a problem in writing without also proposing a solution.

DILIGENCE BASICS – OTHER INTERACTIONS

- Interactions with other individuals who are not your client or your firm's attorneys.

- Preserve attorney-client privilege when interacting with them.

- Observe the line of communication.

- If in doubt, ask a more senior attorney at your firm whether/how you should respond to a communication or request from those individuals.

- **Watch out for who is in the "To:" and "cc:" lines when emailing!**

DATA ROOM

- A data room is a secure online (or physical) location that contains the confidential documents of the target company.

- You must sign an NDA as a condition to gaining access to the data room.

- You may have limited access to data room documents (need to know docs., limited only to viewing images, no printing, downloading or copying allowed).

- The organization and content of the data room will vary with each deal.

- The organization and content of a data room may change significantly even over the course of one deal.

- **Check the data room frequently for additional documents!**

DATA ROOM – ORGANIZATION

- If possible, organize data room like request list.

DATA ROOM – ORGANIZATION

Example data room:

Courtesy of www.intralinks.com

DATA ROOM – MAKING/HANDLING REQUESTS

- Target company may state that request list is overly broad

- Work together to request most relevant documents and if applicable based on stage of negotiations (e.g., are fundamentals acceptable, is system compatible, is IP value commensurate with deal, etc.)

- Thorough and complete due diligence still must be performed

16

DATA ROOM – EXAMPLE RE PATENT DOCUMENTS

For patent diligence purposes, typical minimum request includes the following documents:

- All patents and patent applications assigned to the target, and prosecution histories thereof

- All patents and patent applications in- and out-licensed by target, and prosecution histories thereof

- All patent assignment agreements to which the target is a party

- All patent in- and out-license agreements to which the target is a party

- Employment agreements between the target and the named inventors of the above-mentioned patents

- Freedom-to-operate and validity analyses for the above-mentioned patents

- Publications of subject matter of the above-mentioned patents

- Litigation documents concerning the above-mentioned patents

17

DATA ROOM – PATENT DOCUMENTS

- While you should prioritize review of documents directly related to patents, many other data room documents may be potentially important and may even save you time. For example:

  - A general business PowerPoint may list the patents that the target considers most valuable, and the target's loss-of-exclusivity assumptions for key products.

  - FDA or other regulatory documents can disclose manufacturing processes for the products, which processes the client may want to have analyzed for FTO.

  - The "other contracts and agreements" folder may include end-user IP licenses that do not permit transfer of the target's licensee rights.

  - Patent marking compliance.

18

NON-DATA ROOM DILIGENCE

- Non-confidential resources can be used before the data room is open to make a preliminary assessment of:

  - Chain of title to relevant patents

    - Note that recordation of patent assignments and licenses at USPTO Patent Center and EDGAR is voluntary; thus, not all relevant assignments and licenses may be publicly available.

  - Scope (claim coverage and geographic) of target patent estate

  - Potential patentability/validity issues

  - Potential issues concerning non-employee inventors and third party co-assignees or licensees

19

NON-DATA ROOM DILIGENCE

- Several aspects of IP diligence can be addressed before the data room is open, using non-confidential resources. For example:

SEC Edgar https://www.sec.gov/edgar/searchedgar/companysearch.html	Significant litigation, IP agreements and licenses, information re potential on-sale or public-use bars, regulatory issues
Espacenet https://worldwide.espacenet.com/	INPADOC patent families, US and EP prosecution histories, EP opposition proceedings
USPTO Global Dossier globaldossier.uspto.gov	US and foreign prosecution histories, US continuity data
Docket Navigator	US patent litigation
Darts IP (Clarivate)	Worldwide patent litigation
Derwent Innovation (Clarivate)	INPADOC and DERWENT patent families, projected expiration dates

SUBSTANTIVE ANALYSIS OF TARGET PATENTS

1. Assess Chain Of Title

- Ensure that key patents have clear chain of title from inventors to target by analyzing all relevant agreements.

- Ensure that there are no limitations in any agreements that may impede the acquisition of patents by acquiror.

    - Review target's agreements with third parties (co-assignees, licensees) to ensure that none include restrictions on acquisition of target's patents by acquiror.

    - Resolve any such issues through novations/side letters with third parties.

21

SUBSTANTIVE ANALYSIS OF TARGET PATENTS

2. Assess Scope Of Patent Estate

- Identify all issued patents and pending patent applications, including all family members.

- Identify filing dates and putative priority dates for each patent family.

- Summarize claim and geographic scope for each patent family.

- Note any variation in inventive entity among different members of each family.

- Estimate, if possible, expiration dates for each patent family.

  - Include PTA/PTE where applicable.

  - Assess potential double patenting issues.

SUBSTANTIVE ANALYSIS OF TARGET PATENTS

3.   Assess Strengths And Weaknesses Of Patent Estate

- Review status of pending patent applications and summarize patent office rejections.

- Review status of any pending patent post-grant proceedings.

  - USPTO PGRs/IPRs
  - EPO opposition proceedings

- Review status of any pending patent litigation.

- If requested by the client, conduct FTO and validity analyses, respectively, for target's key products and patents.

FTO AND VALIDITY ANALYSES

- As part of the diligence, your client may ask you to conduct a freedom-to-operate (FTO) analysis of the target's key products.

- Your client may also ask you to conduct a validity analysis of the target's key patents.

- FTO and validity analyses differ in that:

  - FTO analyses focus on the **present:** unexpired or about-to-issue patents owned by a third party that may cover the key products and thus may subject the acquiror to infringement liability.

  - Validity analyses focus on the **past:** prior art that may render the acquired patents invalid for anticipation, obviousness, and/or double patenting. Section 112 issues also should be assessed.

FTO AND VALIDITY ANALYSES

- FTO and validity analyses are related in that:

    - Prior art identified in a **validity search** can potentially be used to address **FTO concerns**.

    - For example, a prior art reference identified when assessing the validity of the target's patent portfolio may also potentially render a problematic FTO patent anticipated or obvious.

FTO AND VALIDITY ANALYSES

- To search for references relevant to either FTO and validity, consider engaging a third party search service.

- Before pulling the trigger:

    - Ensure that you have **client permission** to share relevant information about the relevant products and patents with the search service.

    - Ensure that the service can conduct the search within the appropriate time and budget constraints.

    - Ensure that you and your team have sufficient time and personnel to review and analyze the results of the search.

FTO AND VALIDITY ANALYSES

- Search strategies will vary depending on technology. Some search strategies include:

    - Keyword searches (including synonyms and aliases)

    - Chemical structures

    - Sequence searches for proteins and nucleic acids

- Search strategies often involve a tradeoff between comprehensiveness and relevance.

    - Broad searches are more likely capture important references.

    - But broad searches also are more likely to include irrelevant references that must be weeded out.

FTO AND VALIDITY ANALYSES

- Certain technologies (*e.g.*, chemical compounds) are more amenable to FTO and validity searching than others (*e.g.*, software), wherein nomenclature is less uniform and the relevant prior art can include materials, such as trade show brochures, that is difficult to find.

- Even well-defined technologies such as chemical compounds may pose challenges. For example:

  - Conducting searches for claims to nucleotide sequences that display ">80% homology" to a specific sequence.

  - Conducting searches for a finished compound that can be made using several potentially patented intermediates.

  - Reviewing search results which include patents that claim large genuses of chemical compounds.

28

FTO AND VALIDITY ANALYSES

- The target may have previously conducted its own FTO and/or validity analyses.

- If the target's FTO and/or validity analyses are not included in the data room, consider asking for them.

    - The target, however, may be unwilling to share in view of a potential waiver of attorney-client privilege.

    - "To take advantage of the common interest doctrine the plaintiffs must still satisfy their burden of proving first that the material is privileged and second that the parties had an identical legal, and not solely commercial, interest."

        Katz v. AT&T Corp., 91 F.R.D. 433 (E.D. Pa. 2000)

REPORTING ISSUES TO CLIENT

- Ask the client before putting anything in writing.

- Do not identify problems in writing without also proposing solutions.

- State clearly any assumptions on which you are relying (*e.g.*, assumed patent priority and expiration dates, assumed construction of relevant patent claims).

- State clearly any limitations on searches conducted (*e.g.*, search strategy and search terms used, date restrictions on search results).

- Identify the legal authority upon which you are relying. If there are ambiguities, note them.

REPORTING ISSUES TO CLIENT

Sample reporting letter:

REVIEWING DEAL DOCUMENTS

While the structure of a deal may be dictated largely by non-IP concerns, your client may ask you to review and comment on provisions of the deal documents.

Because you will likely be one the few members of the diligence team that is familiar with patents and the relevant technology, your input on those provisions can be particularly valuable.

REVIEWING DEAL DOCUMENTS

Reviewing definitions:

- Non-IP counsel may not have the expertise or familiarity to determine whether definitions in the document match the scope of key patents and products.

- You will thus be uniquely situated to ensure that the definitions are technically accurate and align with your client's interests.

- You should review/revise definitions with an eye to ensuring that they match what your client intends to acquire or transfer as part of the deal.

- Pay close attention to geographic, temporal and field-of-use limitations in the definitions!

REVIEWING DEAL DOCUMENTS

Reviewing IP assignment and licensing provisions:

- Exclusive or non-exclusive assignment or license?

- Geographic scope?

- Right to transfer, license and/or sublicense included?

- Any carve-out of standard patent rights (make, use, sell, offer for sale, distribute, import)?

- Any field-of-use limitations?

- Any reservation of rights by target, successor or third parties?

- **Limitations on an assignment/license can affect standing to sue.**

34

REVIEWING DEAL DOCUMENTS

Other deal document provisions relevant to patents/IP:

- Ownership of future or joint IP

- Prosecution/litigation responsibilities and cost-sharing

- Key employee/resource sharing

- Representations and warranties

- Non-compete provisions

- Indemnification provisions

- Survival provisions

- Patent/IP schedules

ETHICS: CONFLICTS OF INTEREST

- **Who is the client?** – Company, board, management, or a particular shareholder?

- **Concurrent representation** – Representing buyer and seller in related matters, or advising multiple portfolio companies.

- **Affiliate conflicts** – Handling conflicts in private equity roll-ups or serial acquisitions.

RULE 1.7.

Conflict of Interest: Current Clients

(a) Except as provided in paragraph (b), a lawyer shall not represent a client if a reasonable lawyer would conclude that either:

(1) the representation will involve the lawyer in representing differing interests; or

(2) there is a significant risk that the lawyer's professional judgment on behalf of a client will be adversely affected by the lawyer's own financial, business, property or other personal interests.

(b) Notwithstanding the existence of a concurrent conflict of interest under paragraph (a), a lawyer may represent a client if:

(1) the lawyer reasonably believes that the lawyer will be able to provide competent and diligent representation to each affected client;

(2) the representation is not prohibited by law;

(3) the representation does not involve the assertion of a claim by one client against another client represented by the lawyer in the same litigation or other proceeding before a tribunal; and

(4) each affected client gives informed consent, confirmed in writing.

ETHICS: CONFIDENTIALITY & PRIVILEGE

- **Attorney–client privilege in due diligence** – Sharing diligence results with buyers, bankers, accountants, and consultants.

- **Upjohn warnings in diligence interviews** – Ensuring officers/employees understand who the lawyer represents.

- **Privilege in cross-border deals** – Differences in privilege treatment between U.S. and other jurisdictions.

RULE 1.6.

Confidentiality of Information

(a) A lawyer shall not knowingly reveal confidential information, as defined in this Rule, or use such information to the disadvantage of a client or for the advantage of the lawyer or a third person, unless:

(1) the client gives informed consent, as defined in Rule 1.0(j);

(2) the disclosure is impliedly authorized to advance the best interests of the client and is either reasonable under the circumstances or customary in the professional community; or

(3) the disclosure is permitted by paragraph (b).

"Confidential information" consists of information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential. "Confidential information" does not ordinarily include (i) a lawyer's legal knowledge or legal research or (ii) information that is generally known in the local community or in the trade, field or profession to which the information relates.

(b) A lawyer may reveal or use confidential information to the extent that the lawyer reasonably believes necessary:

(1) to prevent reasonably certain death or substantial bodily harm;

(2) to prevent the client from committing a crime;

(3) to withdraw a written or oral opinion or representation previously given by the lawyer and reasonably believed by the lawyer still to be relied upon by a third person, where the lawyer has discovered that the opinion or representation was based on materially inaccurate information or is being used to further a crime or fraud;

(4) to secure legal advice about compliance with these Rules or other law by the lawyer, another lawyer associated with the lawyer's firm or the law firm;

(5) (i) to defend the lawyer or the lawyer's employees and associates against an accusation of wrongful conduct; or

(ii) to establish or collect a fee; or

(6) when permitted or required under these Rules or to comply with other law or court order.

(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to, information protected by Rules 1.6, 1.9(c), or 1.18(b).

ETHICS: CANDOR & FAIR DEALING

- **Duty to disclose vs. duty of confidentiality** – When lawyers learn material information in diligence that may affect the deal.

- **Negotiation ethics** – Puffery vs. misrepresentation in deal discussions.

- **Ethical limits on drafting** – Aggressive contract terms that may mislead a counterparty.

RULE 4.1.

Truthfulness In Statements To Others

In the course of representing a client, a lawyer shall not knowingly make a false statement of fact or law to a third person.

QUESTIONS?

AI in Tech Transactions

NYIPLA 2025 IP Transactions Bootcamp

October 28, 2025

AI in Tech Transactions

Thank you for joining us today!

- All provided content is the property of NYIPLA and its licensors

- All opinions are personal to the presenters and not any law firm or organization.

- Legal perspectives are general in nature and not intended to provide advice for any particular matter.

- Questions are encouraged!

Data and IP Rights
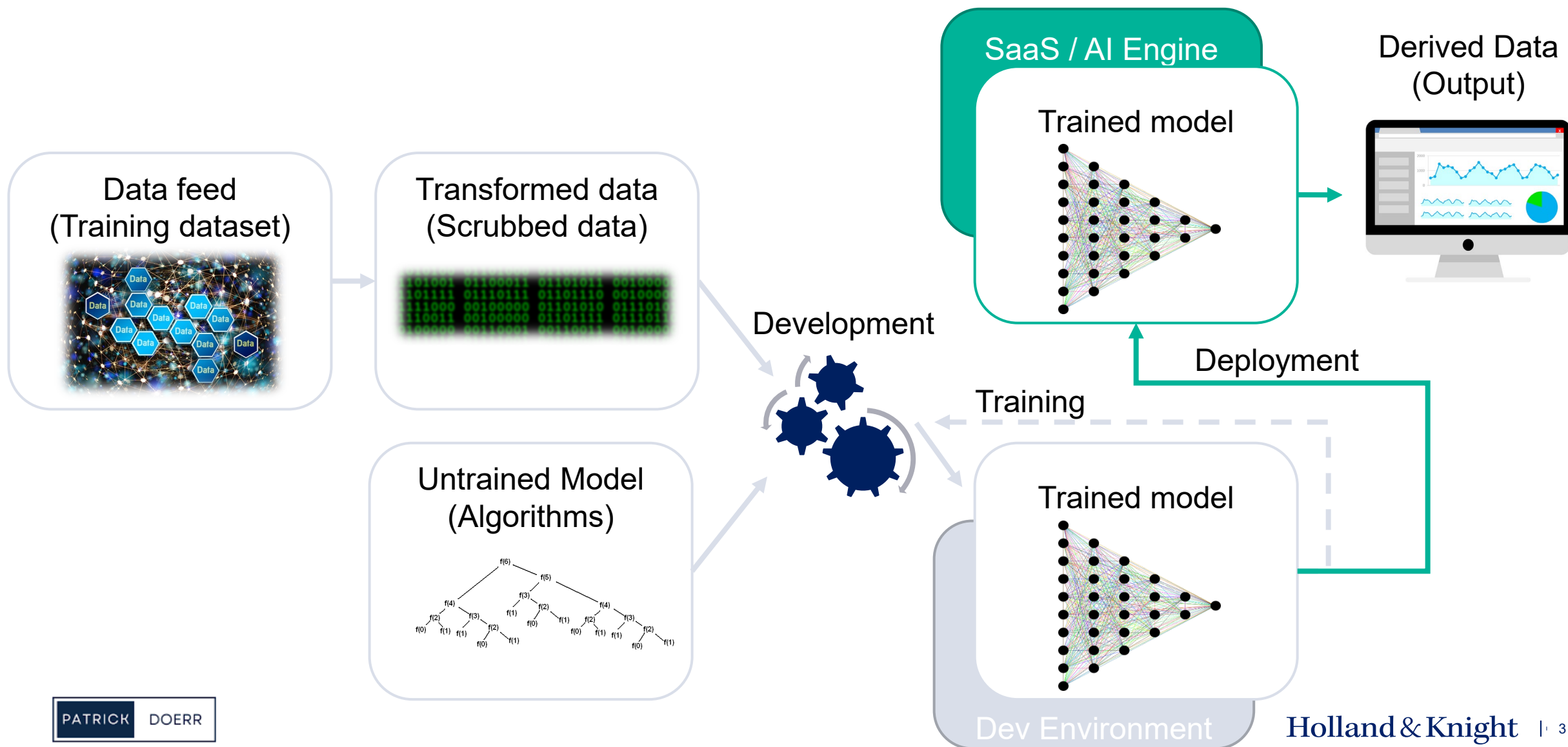
Patents	**Copyrights (databases)**
Trademarks	**Trade Secrets**
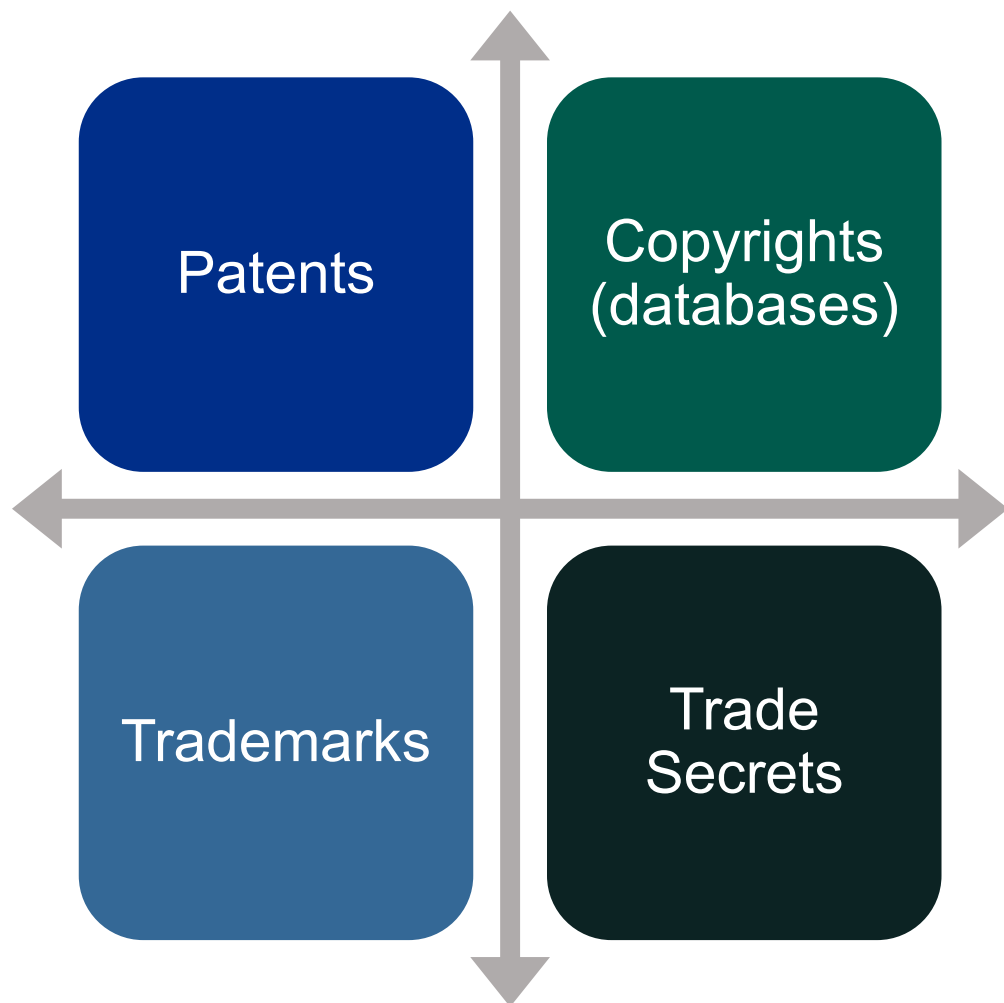
- <u>Federal IP laws</u>: Most licensed data is not protectable within the four categories of IP

- <u>State common laws</u>: offer additional rights in some limited circumstances:

  - Misappropriation (*could apply to proprietary models, has been used for financial models*)

  - Hot news misappropriation (*can sometimes apply to real-time data*)

- <u>Contract rights</u>: can be extremely broad but primarily useful for direct relationships

  - Enforcement challenges for downstream users

 - Can try to mitigate with "flow down" terms; subrogation

PATRICK DOERR

IP Rights in the AI Model

Examples of typical AI development-related risks to be managed by contract

Common "dataset disputes":

- AI training based on customer's labeled dataset (supervised learning)

- AI training based on patterns and inferences drawn from customer's unlabeled dataset (unsupervised learning)

All Provider IP

Developed (in whole or in part) within Project

Developed / acquired outside Project

Derived from Customer's technology or dataset

Not derived from Customer's technology or dataset

Used for purposes of the Project

Not used for purposes of the Project

Jointly developed with Customer

Solely developed by Provider

High blocking risk

Moderate blocking risk

Low blocking risk

Different customer paradigms
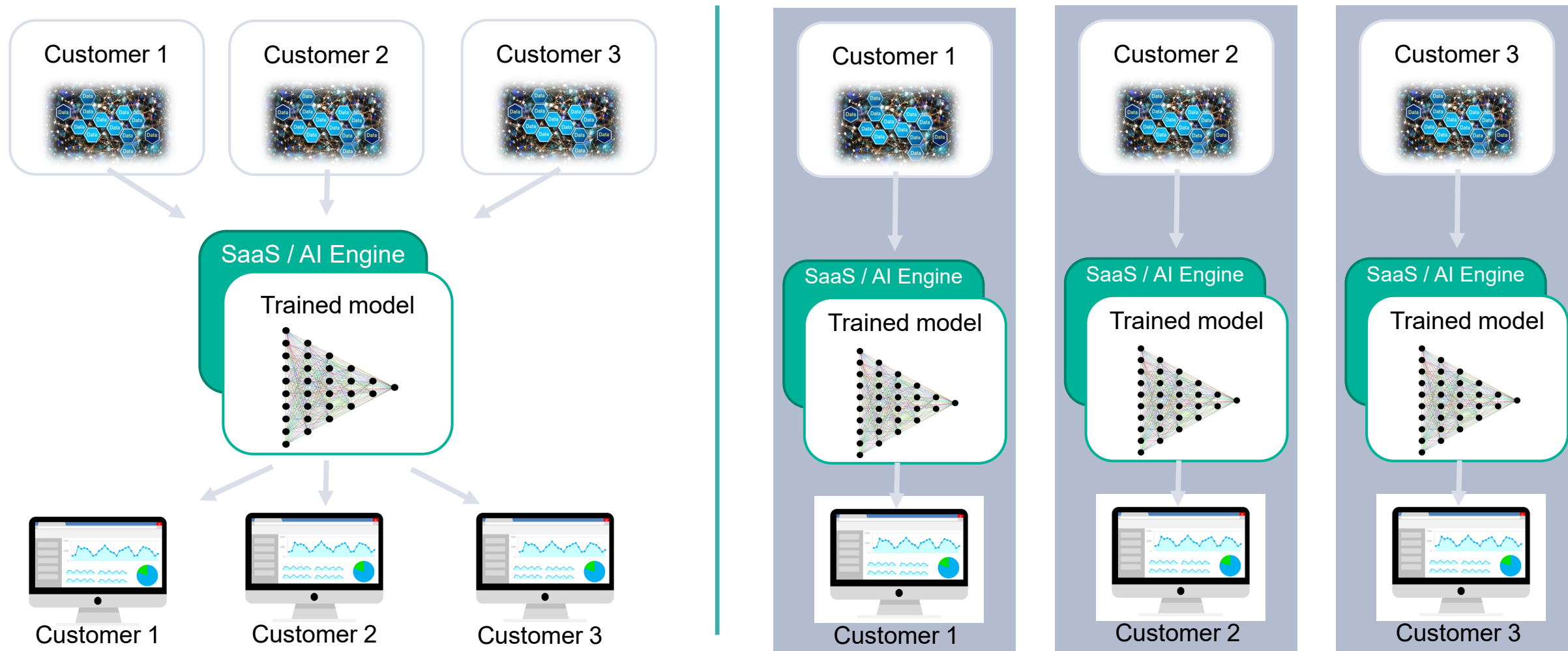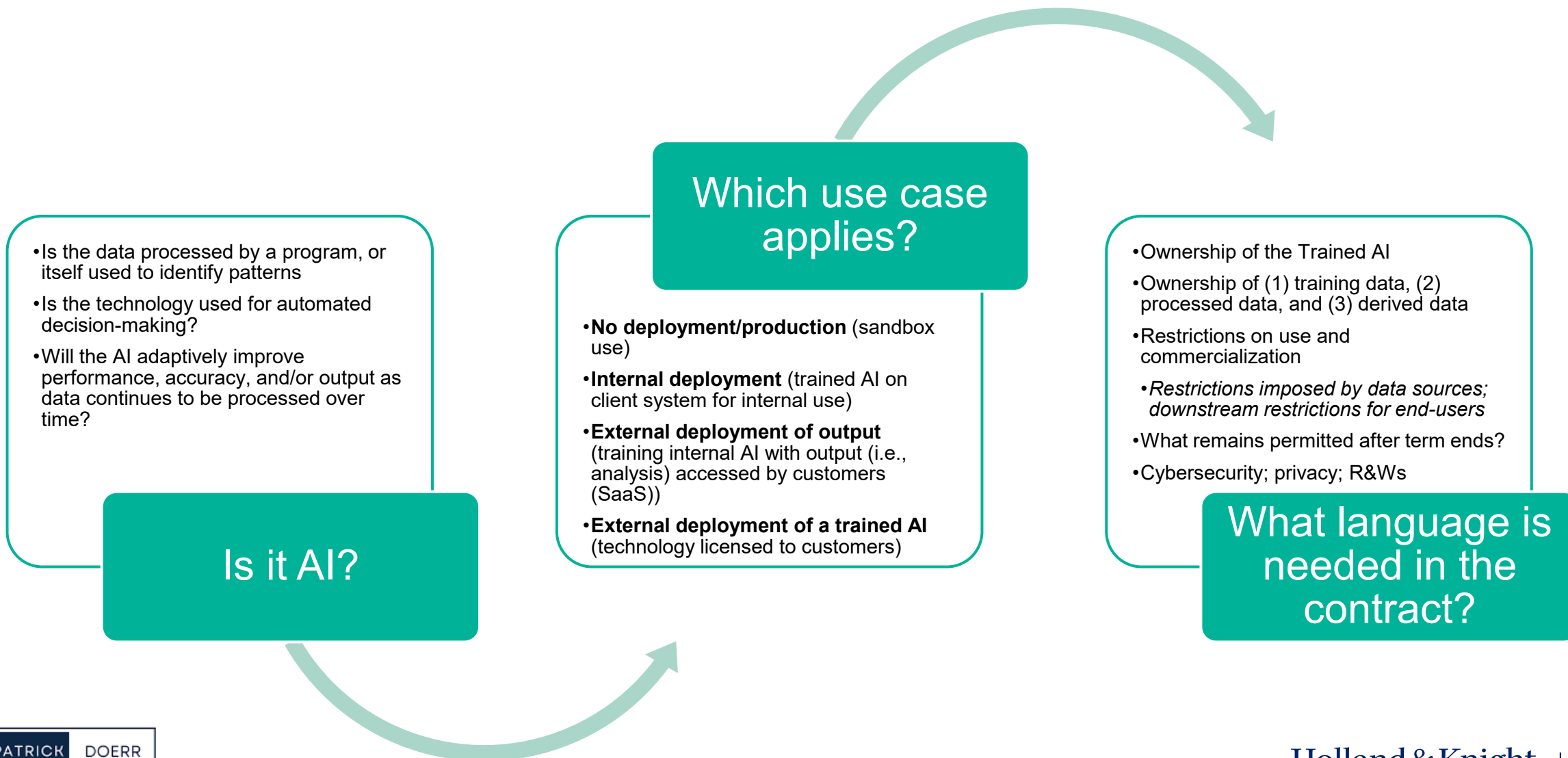
Contracting considerations

- **IP Assets**:

  - Owner v. licensee for the **tech**:

    - Underlying AI tech (software)

    - Trained AI model

  - Owner v. licensee for the **data**:

    - Data feed (Training dataset)

    - Transformed data (Scrubbed data)

      - *Anonymized Input*

    - Derived Data (Output)

      - *Anonymized Output*

Contracting considerations

- **Scope of rights (for <u>each</u> party):**

  - Duration (rights during term, and rights after termination)

  - Territory (US v. worldwide)

  - Permitted "fields of use" (*e.g.,* "no consumer credit decisions")

  - Internal v. External use:

    - "internal business use only" v. customer-facing, commercialization rights

- **Implementation:**

  - Consider cloud vs. on-premises applications – "*bring the data to the processing … or the processing to the data*"?

    - Information security controls

    - Service level obligations (SLAs)

    - Potential loss of control over AI tech v. data

Contracting considerations

- **Compliance and Risk Allocation**

  - Data Privacy

    - De-identification obligations

    - Consent and cross-border transfers

    - Do contract terms align with legal obligations (*e.g.,* CCPA, GDPR, VPPA)?

  - Functionality

    - "Substantial compliance with documentation" requirements

    - Acknowledge probabilistic nature of output

    - Risk allocation for bias and data quality

    - Managing transparency and explainability in automated decision-making (the "black box")

Contracting considerations

- **Compliance and Risk Allocation**

  - Liability and Indemnity – beware of the "*AI Carveout*"

    - Liability disclaimer and liability shifting

      - Data inputs

      - Data outputs / automated decision-making

    - Indemnity for IP infringement and other claims

  - Impact on the standard provisions

    - Legal compliance (new and evolving AI laws + traditional obligations)

    - Subcontractors (e.g., OpenAI)

    - Audit rights, Insurance coverage, Response to 'incidents'

  → All relevant in M&A and other due diligence projects

Mark Francis

Mark Francis
Partner
Holland & Knight LLP
New York

Mark Francis is a tech and data partner at the law firm Holland & Knight LLP in New York, with a practice spanning legal compliance, investigations, litigation, and a wide array of transactions. In connection with his practice, Mark advises on cybersecurity, federal, state, and foreign privacy laws, information governance, third-party risk management, artificial intelligence, AdTech, data strategy, intellectual property and quantum computing. He frequently counsels clients in response to data breaches and other incidents, guiding them through internal investigations, regulatory inquiries, and legal disputes.

Mark has a background in computer science and telecommunications, and received his JD/MBA from Fordham University. He is a Certified Information Systems Security Professional (CISSP) and Certified Ethical Hacker (CEH), as well as an IAPP Privacy Law Specialist and Fellow of Information Privacy. Mark recently served on the U.S. Department of Homeland Security (DHS) Data Privacy and Integrity Advisory Committee (DPIAC), providing privacy-related advice at the request of the Secretary of Homeland Security and the DHS Chief Privacy Officer. Mark is currently serving on the IAPP's Certification Advisory Board, at the AI Policy Consortium on Law and Courts (a joint initiative of the National Center for State Courts and the Thomson Reuters Institute), and on Practical Law's US and Canada Data Privacy & Cybersecurity Advisory Board.

For more information, please visit https://www.hklaw.com/en/professionals/f/francis-mark-h or https://www.linkedin.com/in/markhfrancis/.

Mark Doerr

Mark Doerr
Co-Managing Partner
Patrick Doerr
New York

Mark Doerr is the Co-Managing Partner of Patrick Doerr, where he leads litigation and intellectual property matters with precision and creativity. Mark has more than 15 years of experience representing clients in high-stakes disputes across the United States. Mark is known for navigating challenges with clarity and understanding, and for delivering outcomes that matter.

His practice spans litigation, intellectual property, and entertainment, with a particular focus on New York City's creative industries. Beyond the courtroom, Mark draws professional inspiration from electronic music production and performance, a passion that mirrors his approach to law: innovative, technical, and always focused on empowering creators to create and communities to thrive.

Mark holds a BA from the University of Illinois at Urbana-Champaign and a JD from Columbia Law School.

Questions?

Use of AI Notetakers in Communications with Counsel

Overview: AI Notetakers

- Increasingly used to transcribe and summarize meetings with speed and efficiency.

- Digest and memorialize complex discussions

- Client's favorite for meetings involving in-house and outside counsel.

- Balance value against important considerations regarding the preservation of confidentiality and attorney-client privilege.

- Attorneys should be mindful of these risks and take appropriate steps to ensure that the use of AI notetakers does not compromise privileged communications or impair their ability to effectively advise clients.

MORRISON FOERSTER

AI Notetaking Risks – Overview

- Disclosure of attorney-client communications to third parties.

- Use of meeting data for model training.

- Transcription inaccuracies or hallucinations.

- Improper data storage or access controls.

- Failure to meet state recording consent requirements.

Confidentiality & Privilege Risks

- **Risk:**

  - AI vendors may reuse meeting content, risking privilege waiver.

  - AI introduces novel scenarios in which privileged communications, or insights derived from them, could be exposed.

  - Arise from how AI systems are configured, the nature of vendor access, or the ways in which outputs are shared or reused.

- **Mitigation:**

  - Check provider data-sharing practices and disable training use.

  - Avoid unapproved or consumer-grade AI tools for legal meetings.

MORRISON FOERSTER

Accuracy and Reliability Risks

- **Risk:**

  - AI can misstate or invent content ('hallucinations').

  - From transcription inaccuracies to more complex "hallucinations" that may alter the substance of attorney-client communications.

  - Omission or creation of content, or the unintended emphasis or de-emphasis of certain points.

- **Mitigation:**

  - Review and verify transcripts before reliance.

  - Mark AI-generated outputs as drafts until confirmed.

Data Management & Storage

- **Risk:**

  - Unauthorized access to AI-generated transcripts.

  - Providers may not prioritize secure deletion or retention controls specific to privileged material, as these concerns are unique to legal contexts.

- **Mitigation:**

  - Ensure materials are linked to the correct client file.

  - Review provider's deletion and retention practices.

  - Ensure secure deletion of meeting content post-processing.

Recording Consent & Legal Compliance

- Some U.S. states require all-party consent for recording.

- AI notetakers may not automatically provide notice.

- Provide explicit verbal or written notice at meeting start.

- Non-compliance can lead to liability or ethical issues.

Recap: AI Notetaking Best Practices

- Provide clear notice of recording to all participants.

- Use only approved AI notetakers with data protection controls.

- Review provider's privacy and data-use terms.

- Execute a data processing agreement identifying provider obligations.

- Follow organizational vendor management procedures.

- Manually review all outputs before use or distribution.

- Store materials securely and limit access to authorized personnel.

- Use discretion—avoid AI notetakers for highly sensitive discussions.

Key Takeaways

- AI notetakers can improve efficiency but pose privilege and compliance risks.

- Vet vendors carefully and use human review for accuracy.

- Ensure strong data governance and clear recording consent processes.

- Apply professional judgment to determine when AI tools are appropriate.

Boris Segalis

Partner | New York

+1 (212) 336-4260

bsegalis@mofo.com

Education

- Georgia Institute of Technology, B.S.
- New York University School of Law, J.D.

Boris Segalis is a partner in Morrison Foerster's Privacy + Data Security Group. For over a dozen years, he has counseled clients on privacy and cybersecurity issues in the context of strategic product advice, corporate transactions, and regulatory investigations.

Boris regularly advises clients on the development and implementation of data-driven products and services, on global privacy and cybersecurity compliance, and on handling cyber incidents affecting companies and users globally. Boris defends companies in U.S. federal, state, and global privacy and cybersecurity investigations, including representing clients in front of the Federal Trade Commission (FTC), the New York and California attorneys general, and foreign regulators. His practice also focuses on advising clients on the requirements of a variety of U.S. and global privacy laws, including the California Privacy Rights Act (CCPA/CPRA) and other U.S. state privacy laws, the General Data Protection Regulation (GDPR), the EU-U.S. Data Privacy Framework, and the EU's ePrivacy Directive.

Boris counsels clients ranging from emerging to late-stage to public companies across industries, including technology, data brokerage, AI, financial services and Fintech, crypto, life sciences, consumer services, e-commerce, AdTech, media, and others. For seven consecutive years, Boris has been individually recognized by *Chambers USA* in the Privacy & Data Security category and is recognized *by Chambers Global* for Privacy & Data Security – USA. He has also been recognized by *The Legal 500* as a leading lawyer in cyber law (including data privacy and data protection). *Crain's New York Business* has previously included him in its 40 Under 40 list.

Boris is a Certified Information Privacy Professional (CIPP/US) through the International Association of Privacy Professionals (IAPP), has previously served as co-chair of NYC IAPP KnowledgeNet, and served on the IAPP's Research Board. Boris currently chairs the UJA Privacy and Cybersecurity Group. Boris also is an adjunct professor at Vanderbilt University School of Law.

Rankings

***Chambers USA**, 2014 – 2024*

Ranked in Nationwide: Privacy & Data Security

***Chambers Global**, 2015 – 2025*

Ranked in Privacy & Data Security

***The Legal 500 US,** 2020 – 2024*

Recognized as a Leading Lawyer in Cyber Law: Data Privacy and Data Protection

MORRISON FOERSTER