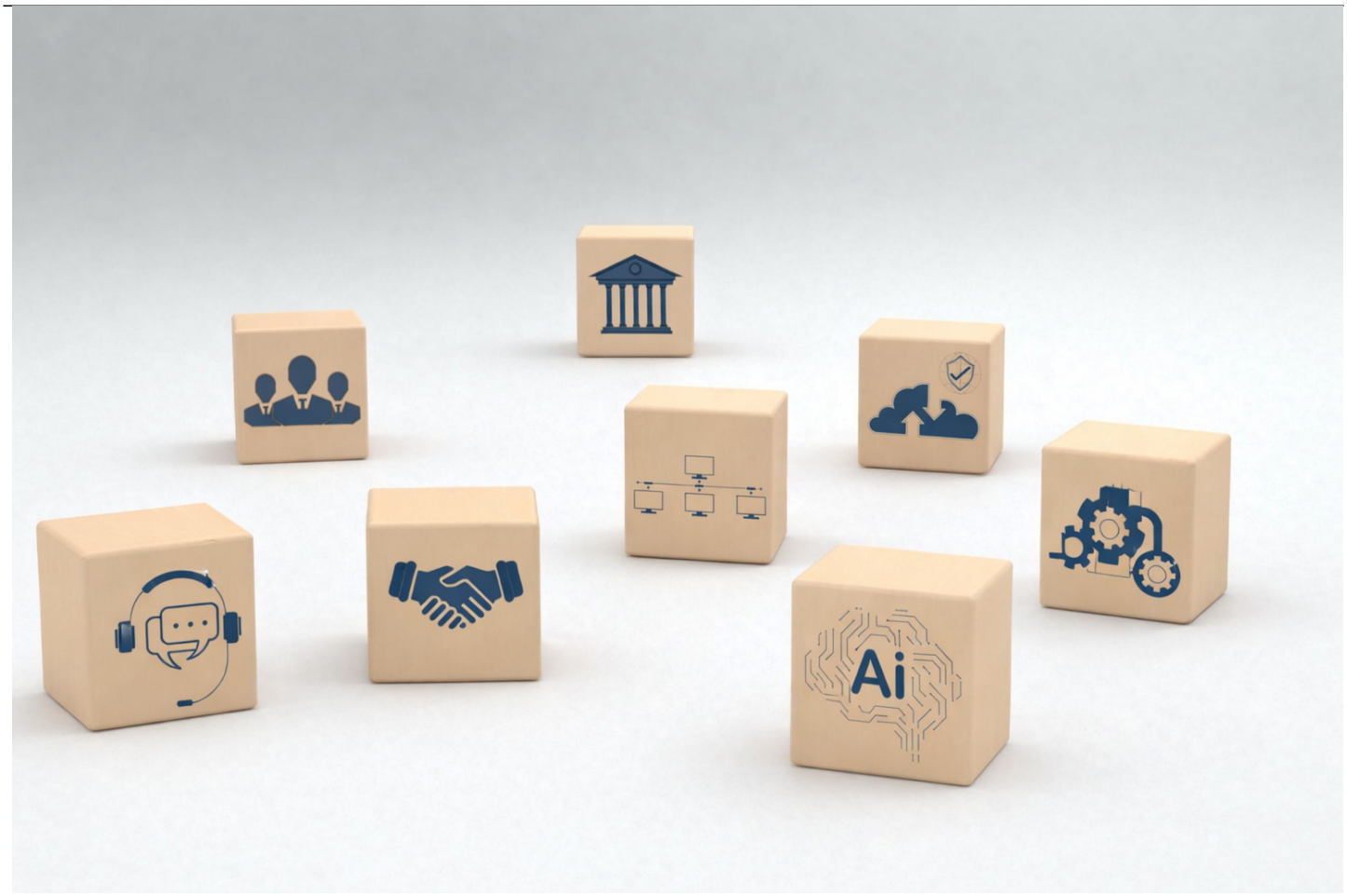
Why Legal’s Cross-functional Role Is the Key to Scalable Enterprise AI

Technology, Privacy, and eCommerce



Banner artwork by Fit Ztudio / *Shutterstock.com*

Cheat Sheet:

- **Legal sees across the enterprise.** Unlike siloed teams, Legal works horizontally across departments, giving it a unique view of AI workflows, data flows, and risk intersections.
- **AI requires unified governance.** Scalable enterprise AI fails without consistent governance, permissions, and oversight embedded across tools, teams, and use cases.
- **Permissioned AI enables trust.** AI systems that inherit enterprise access controls allow innovation without expanding data exposure or violating contractual and regulatory obligations.
- **Legal balances risk and speed.** By translating the enterprise's obligation graph into practical guardrails, Legal helps organizations move fast with AI — without breaking trust or compliance.

Note: This article is Part 2 in a two-part series on why Legal sits at the center of successful enterprise

AI adoption. Read Part 1 here.

AI doesn't live inside a single department. It cuts horizontally across workflows, systems, obligations, and data flows. That means the function best positioned to lead AI strategy is one that already works horizontally. That function is often Legal, along with partners in Finance (to see what tools are being purchased) and IT (to see what SaaS platforms are being accessed from company laptops and systems). Legal tends to have a "bird's eye view" across most — if not all — departments, and routinely observes hotspots when legal review is requested for a situation or potential dispute.

Most teams collaborate episodically — Sales loops in Security when needed for a deal, Product checks with Compliance before a release, HR consults Finance on a new expense policy. Legal, by contrast, collaborates continuously, often daily, with all of these departments. For example, in the experience of the authors, the following functional groupings are common:

- The Transactions Legal team (GTM contracting team) is tightly aligned with Sales and Deal Desk (Finance), and Channel Partner teams.
- The Product Legal team (IP, privacy, product compliance, licensing, inbound licensing) is tightly aligned with Engineering, Product Management, Tech Alliances, Direct Procurement, Support, Marketing, and many other teams.
- The Employment Legal team is tightly aligned with the People/HR team, local regional managers, and more.
- The Corporate Legal team is tightly aligned with Finance (local entities, Board matters, taxation), People/HR (for stock compensation, etc.), and more.
- Every customer contract touches Sales, and often Product, Security, and Finance.
- Changes in company policies can implicate Finance, Security, HR, IT, and Compliance.
- Data breach investigations require coordination between the owner of the impacted service and Leadership, Data, and Security.
- Regulatory changes can draw in Product, Finance, Security Engineering, Operations, and Marketing all at once.

In addition to the practice specific relationships outlined above, Legal routinely quarterbacks cross-functional tasks such as RFPs, due-diligence reviews, privacy assessments, and security questionnaires. These processes require tightly coordinated input from Engineering, Security, Product, IT, HR, Finance, and Procurement. These activities expose Legal to the operational realities of the business: where information resides, which tools are used by each team, where workflows slow, and where obligations intersect. This visibility provides Legal with a view on the categories of data each team holds and uses: trade secrets, confidential information shared under NDA, code and product technical data repositories, personally identifiable information (PII), and special categories of

data (health, financial, and sensitive personal information).

Through this constant engagement, Legal develops a uniquely comprehensive view of the business: a deep understanding of how work moves through the enterprise, and where data flows across departments and tool stacks. It sees where bottlenecks form, where obligations conflict, where data becomes trapped in silos, and where privacy and security exposures emerge. It also sees where AI can create leverage without introducing new forms of risk.

This is where strongly permissioned AI systems become essential. AI is only safe when it operates on top of the same permissions, entitlements, and access controls that govern the rest of the enterprise. When AI inherits those controls, thereby surfacing only the data an employee already has the right to see, then Legal can enable AI deployment with confidence, knowing it won't expand access, circumvent restrictions, or inadvertently expose sensitive information. Permissioned AI turns Legal's deep cross-functional insight into actionable guardrails: enabling innovation while ensuring every model, query, and workflow stays inside the organization's data and contractual boundaries.

> AI is only safe when it operates on top of the same permissions, entitlements, and access controls that govern the rest of the enterprise.

Legal's enterprise-wide vantage point becomes especially valuable when understanding and determining how AI is entering and spreading across the organization. Because Legal reviews inbound AI vendor contracts, it often becomes the primary function with a comprehensive line of sight into the organization's full AI footprint. There is an opportunity to partner with Finance teams to identify any shadow-AI spend occurring on company credit cards, and ensure appropriate contractual protection and governance are in place. There is also an opportunity to partner with IT to identify which SaaS tools data is flowing to or from, regardless of whether those tools are paid (which Finance/Legal should see) or free (which often remain undetected by Finance/Legal). With this partnership and input, Legal can identify issues that often remain invisible to individual business units:

- duplicative pilots solving the same problem;
- inconsistent data rights and training rights across vendors;
- misaligned or unapproved use cases;
- shadow AI tools deployed outside governance frameworks; and
- privacy blind-spots due to unofficial use of tools with personal data.

Many AI initiatives fail not because the underlying models are insufficient, but because organizations unintentionally create parallel, incompatible versions of the same capability, each governed by

different contracts, data flows, and assumptions about risk. Left unchecked, this leads to tool sprawl, fragmented governance, and architectural inconsistency that make scaled AI deployment challenging or impractical. It is also important for Legal to educate new employees and train or refresh existing employees, providing a baseline knowledge on privacy, confidentiality, AI governance, and employee policies around use of AI tools both within and outside of company systems.

> It is also important for Legal to educate new employees and train or refresh existing employees, providing a baseline knowledge on privacy, confidentiality, AI governance, and employee policies around use of AI tools both within and outside of company systems.

Legal is one of the few functions with both the oversight and the authority to recognize these patterns early and steer the organization toward consolidation and coherence before the costs and risks of unmanaged AI sprawl become irreversible.

In an environment where AI reshapes workflows across the entire enterprise, success depends on a function capable of coordinating horizontally, interpreting conflicting obligations, and ensuring systems operate under a unified framework. Legal is uniquely equipped to play that role, and AI strategy only succeeds when someone does. It is essential to build governance, trust, accountability, and explainability into any workplace AI transformation effort, both for compliance with laws (EU GDPR, EU AI Act, US State laws, and more) and to maintain customer trust regarding how their data may be processed.

Legal knows how to balance risk and innovation — across the entire enterprise and innovation

Every organization faces the same tension with AI: move fast enough to capture opportunity, but not so fast that you create unacceptable risk. Most teams experience that tension only within their own lane — Product sees product risk, Security sees security risk, HR sees people risk. Legal is one of the few functions that routinely sees the intersections.

Lawyers make judgment calls every day that depend on understanding multiple functions at once: how a product feature interacts with regulations, how contract terms shape Sales strategy, how a data workflow touches Security, or how an automated decision impacts HR and Compliance. Legal's work is inherently cross-functional, so its risk calculations tend to reflect that broader view.

The speed at which AI coding assistants enable developers to build software quickly, marketers to

generate media content in minutes rather than days, and product teams to launch new features in days instead of weeks or months is a double-edged sword. AI enables all these users to arrive at solutions faster, but often doing so bypasses traditional checkpoints such as engineering design reviews, product feature gate reviews, marketing content verification, and more. This can lead to something shipping quickly without compliance checks, validation of claims, or pausing to question whether a solution is the right or most appropriate one for the market, jurisdiction, or audience.

> AI enables all these users to arrive at solutions faster, but often doing so bypasses traditional checkpoints such as engineering design reviews, product feature gate reviews, marketing content verification, and more.

The complexity of AI amplifies the need for an integrated perspective and global governance across the company. New exposures rarely sit neatly within one department:

- A model may generate output that accidentally creates contractual commitments, such as the chatbot that 'sold' a car for a dollar.
- Automated decisions may trigger regulatory obligations no one has operationalized, particularly with the fast-moving pace of new global and US AI regulations.
- Training data rights across vendors may be inconsistent or ambiguous.
- Inferred data may fall outside established privacy frameworks.
- Multiple AI systems may interact in ways that make outcomes difficult to explain or defend, running counter to the GDPR principles of transparency and explainability (Article 5), rights of deletion (Article 16), and/or correction (Article 17).

These are not theoretical issues. They are happening today: chatbots offering refunds that violate the master agreement; unapproved AI note-takers capturing privileged or confidential information; AI-generated logs complicating incident response because no one can fully explain how the output was produced, or even hallucinations present in AI-generated logs or summaries.

Legal is often the first function to see how these issues collide across teams, not just within them. When Legal is involved early, it can translate fragmented concerns into a cohesive strategy. How do we build this feature so it aligns with our contractual obligations and global privacy regulations? How do we automate this step while preserving required review, particularly with a human in the loop? What evidence will we need to have ready to present to regulators or customers if this output is ever challenged? Early Legal involvement turns these questions into a holistic strategy while there is time to plan a well-reasoned response and process, not an emergency or patchwork fix cobbled together under regulatory scrutiny.

> When Legal is involved early, it can translate fragmented concerns into a cohesive strategy.

The organizations that will move fastest and most safely in the AI era are the ones that treat Legal not as a brake but as the function responsible for keeping both risk and progress in balance, while moving at AI-speed. In a world where AI reshapes decisions, speed, and accountability all at once, that balancing role becomes foundational to scaling AI responsibly. Just as a champion race-car driver employs the right balance of speed and control to stay ahead of the pack, companies embracing AI must blend speed, oversight, and user empowerment to excel in their fields.

Legal understands the enterprise obligation graph — and AI can't scale without it

Every enterprise runs on an invisible system that determines what it can and cannot do: its obligation graph. This graph is the network of contractual promises, regulatory requirements, data-use restrictions, privacy rules, retention mandates, audit obligations, and operational commitments the company has accumulated over time. Sometimes it also includes tribal knowledge within the business that may not be in any formal policies or procedure documents, but is simply "the way it's done" at a given company.

Most functions only see their slice of that graph. Legal typically sees most (and, in some cases, all) of it — and interprets how each obligation affects every other.

This matters because AI doesn't run inside functional boundaries such as departmental organizational charts. It runs inside the obligation graph.

- A training dataset must respect contractual use restrictions.
- An automated decision may create regulatory consequences.
- A model's output can become a warranty, admission, or unintended commitment.
- Inferred data may trigger employment or privacy protections, even if the user or data subject is unaware of these.
- AI-generated logs may become discoverable evidence or regulated records, even if unintentionally so.

Legal, often in partnership with its IT and business system owner counterparts, is well suited for translating the obligation graph into implications for AI:

- Which data sources have training rights?
- What use cases break existing promises?
- What jurisdictions impose heightened review?

- What evidence must be generated and retained?
- When is a human-in-the-loop legally mandatory?
- What systems contain special categories of data (GDPR Article 9.1) and which regulatory obligations are triggered if AI acts on this data?

When these obligations are invisible, AI initiatives drift into misalignment, stall, or get shut down. When Legal, in partnership with IT and business counterparts, maps the obligation graph and embeds it directly into workflows, AI becomes scalable, defensible, and aligned with the company's commitments.

> When Legal, in partnership with IT and business counterparts, maps the obligation graph and embeds it directly into workflows, AI becomes scalable, defensible, and aligned with the company's commitments.

This is the structural reason Legal is indispensable to AI strategy: it is often the primary function that knows how the enterprise's obligations interact, and how to keep AI inside the boundaries of what the organization is allowed to build.

Legal's emerging leadership mandate in the AI era

AI is forcing organizations to confront a simple truth: no single function can scale AI alone. Every meaningful AI use case crosses boundaries — between Product and Security, HR and Compliance, Engineering and Finance, IT and Operations. The work is cross-functional by design, and Legal already lives at those intersections.

Legal's value in this context isn't about claiming ownership of AI strategy. It comes from the day-to-day work of helping teams interpret obligations, understand constraints, and navigate situations where requirements overlap or pull in different directions. That perspective can make it easier for cross-functional groups to stay smoothly aligned as they explore new tools and approaches. And as AI reshapes more decisions and workflows, that steadiness becomes one of the most reliable ways to keep innovation and governance connected. Trust, explainability, governance, and oversight are all skills Legal is adept at, and in the new age of AI, they're what unlock safe, productive, and efficient enterprise AI adoption at scale. When those foundations are in place, employees trust and rely on the tools, customers see consistency, rather than surprises, and the CFO sees investment rather than exposure. Happy users, happy customers, and happy CFO. It's difficult to argue with that level of alignment.

Join ACC for more AI insights!

Michael T. Moore

Chief Privacy Officer

Lacework, Inc.

Michael T. Moore is the vice president, privacy and IP at Lacework, Inc. a cloud security company in Mountain View, CA. He has responsibility for privacy and cybersecurity, procurement, product counseling, transactional support, patents and intellectual property strategy, open-source software, and other matters. Moore is a seasoned attorney with more than a decade of privacy, cloud, transactional, software and hardware counseling and patent and IP experience, which follows his technical career in logic design and software engineering.

Previously Moore was the vice president, products and IP at Pure Storage in Mountain View. Pure Storage has been recognized twice by The Recorder for In House Legal Department of the Year in 2016 and 2017 for IP Strategy, and also recognized for Litigation (2016) and for Data Security (2017), and Legal Operations (2019) which fall into Mr. Moore's area of responsibility. In 2018 Pure Storage was named by the Association of Corporate Counsel as Value Champion Award Winner.

Before joining Pure Storage, Moore was the vice president, intellectual property and deputy general counsel, of Rambus. He has also worked in-house at Symantec, and he started his attorney career as an associate at the law firm of Morgan, Lewis and Bockius involved in patent prosecution and trade secret litigation. Prior to this Moore spent almost a decade in the semiconductor industry as an engineer and patent agent.

Moore holds a JD and MBA from Santa Clara University, and BSEE (B.Eng) from the University of Limerick, Ireland. He speaks at PLI, ACC, and other events and has published in *Law360*, *ACC Docket*, *Corporate Counsel*, *Intellectual Asset Management*, and other legal journals. He holds 10 US issued patents from his engineering work.

Rebbea Hinds

Head of the Work AI Institute

Glean Technologies, Inc.

Rebecca Hinds is the Head of the Work AI Institute at Glean, where she leads research on how AI is reshaping the way people work. She earned her B.S., M.S., and Ph.D. from Stanford University. Her research and work focus on how emerging technologies — especially AI — change organizational behavior, collaboration, and performance. Her research and insights have appeared in outlets such as *Harvard Business Review*, *The New York Times*, *The Wall Street Journal*, *Forbes*, *Inc.*, and *Time,* as well as top academic outlets like *Organization Science* and *CSCW*. Hinds is a co-instructor for the CNBC *Make It* course *How to Use AI to Be More Successful at Work*, and is the author of *Your Best Meeting Ever*, named a Next Big Idea Club “must-read.”