Navigating 2025: Key trends shaping the Technology Sector

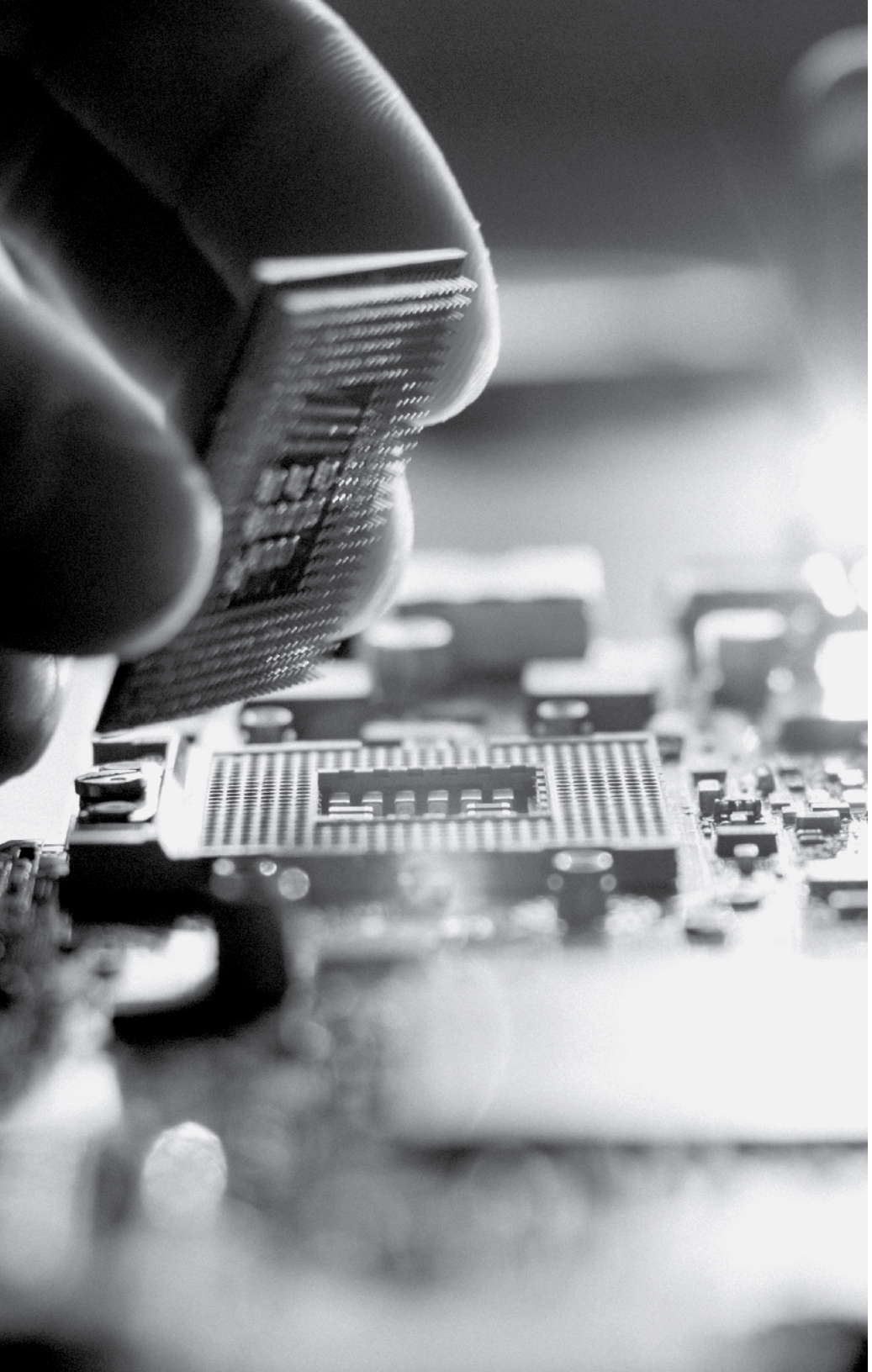
FASKEN

Own tomorrow

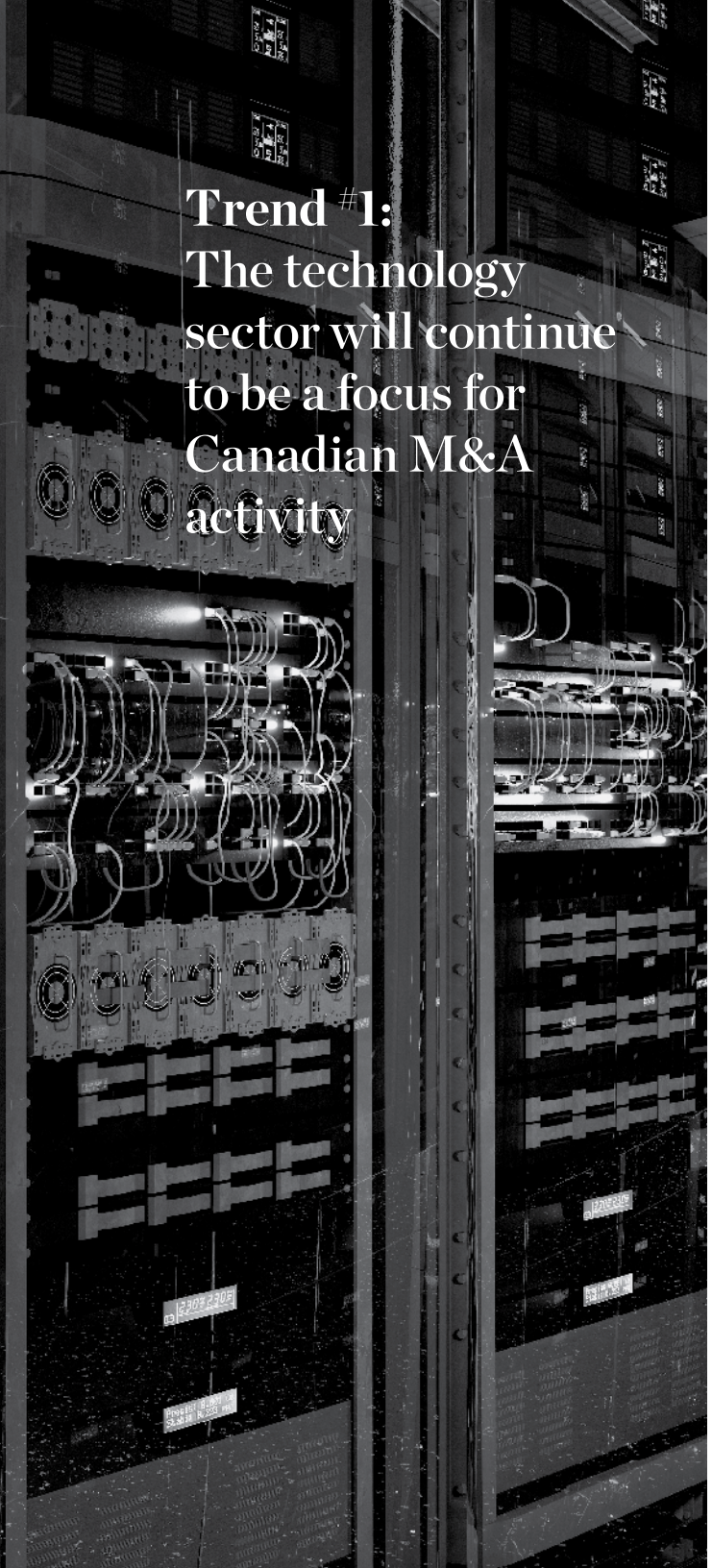
Navigating 2025: Key trends shaping the Technology Sector

In 2025, technology providers and technology users are navigating a complex landscape filled with both challenges and opportunities. Market dynamics driven by technology innovation, the push for profitability, shifting risk attitudes, a focus on environmental, social and governance (ESG) initiatives, heightened geopolitical and cybersecurity concerns and new legislative and regulatory changes are reshaping the face of IT.

To help you navigate these changes, Fasken's Technology Law team has prepared this guide highlighting key trends confronting the Canadian technology sector in 2025.



Contents



Trend #1: The technology sector will continue to be a focus for Canadian M&A activity

Technology deals are expected to remain a focal point for M&A activity in 2025. The rise in Tech M&A is expected to be driven by innovation in emerging industries, the ongoing efforts of industry players to enhance their artificial intelligence (AI) capabilities, and the anticipated loosening of regulatory constraints for the tech sector as a probable outcome of the new US administration.

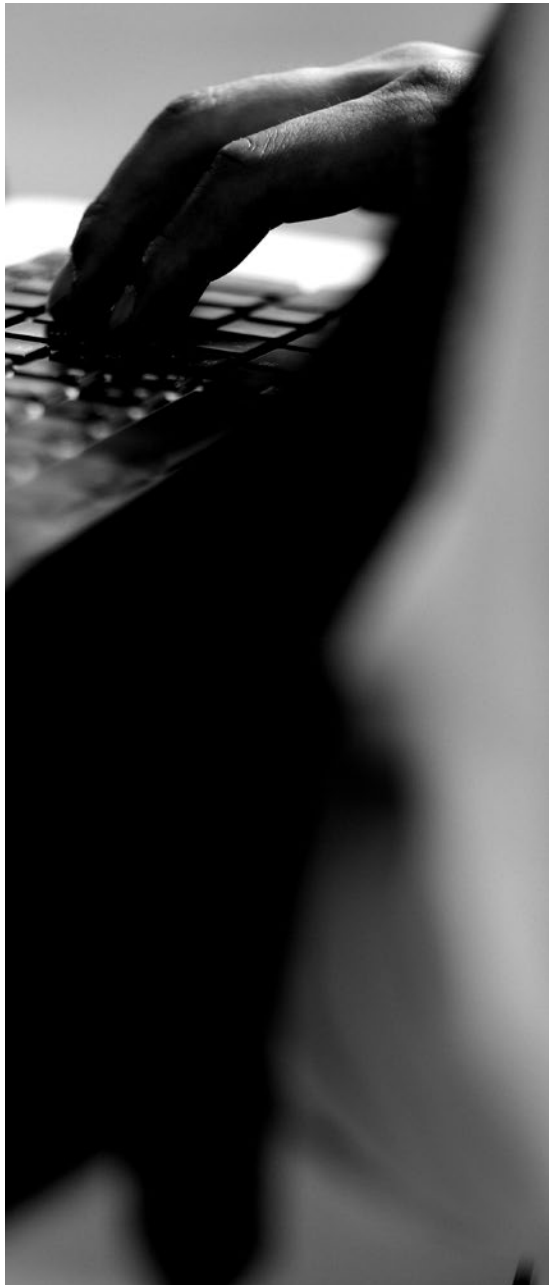
EMERGING THEMES AND OPPORTUNITIES IN TECH M&A

An analysis of M&A activity in the information technology sector in Canada over the past several years[1] has revealed the following themes and opportunities:

- **Business Productivity Software and IT Outsourcing**: These areas continue to dominate deal volumes, reflecting organizations' increasing focus on tools and services that enhance efficiency and address operational complexity.
- **Software as a Service (SaaS)**: SaaS remains the top vertical for Tech M&A, with steady growth in deal volume over the past three years. This trend underscores the sustained demand for scalable, cloud-based solutions that support hybrid work environments and enterprise-level efficiencies.
- **Application-Specific Semiconductors**: This industry vertical strengthened significantly in 2024. Although deal volumes are relatively low, there has been noticeable growth. This reflects the importance of semiconductors in supporting advancements in AI and other data-intensive technologies.
- **Artificial Intelligence & Machine Learning**: This sector continues to be a key industry vertical, accounting for 7.03% of Tech M&A in 2022, rising to 12.66% in 2023, and maintaining a strong presence at 11.79% in 2024, despite a broader decline in overall deal volume. This growth highlights AI's pivotal role in driving innovation and value creation across industries.

It is important to note that these verticals are complemented by other related verticals and are not the exclusive focus of M&A. For example, the rise in semiconductor deals will complement the continued focus on strategic minerals for the North American market.

1. Data in this analysis is sourced from PitchBook, reflecting M&A and change of control transactions in Canada within the information technology sector for 2022, 2023 and 2024.



CONSIDERATIONS FOR AI-FOCUSED TECH M&A

The integration of AI into business models has fueled M&A activity, presenting both opportunities and unique challenges. These challenges—ranging from model accountability to regulatory scrutiny—are shaping the due diligence process and the representations and warranties in acquisition agreements.

Due Diligence

The relative newness of AI necessitates a more comprehensive due diligence process to properly assess the value and risks of a target. For an AI target, tailored approaches are required to cover AI-specific issues such as data quality, data rights, and compliance with evolving regulations. This includes evaluating the integrity and legality of data used for training AI models and ensuring the models' accuracy and reliability.

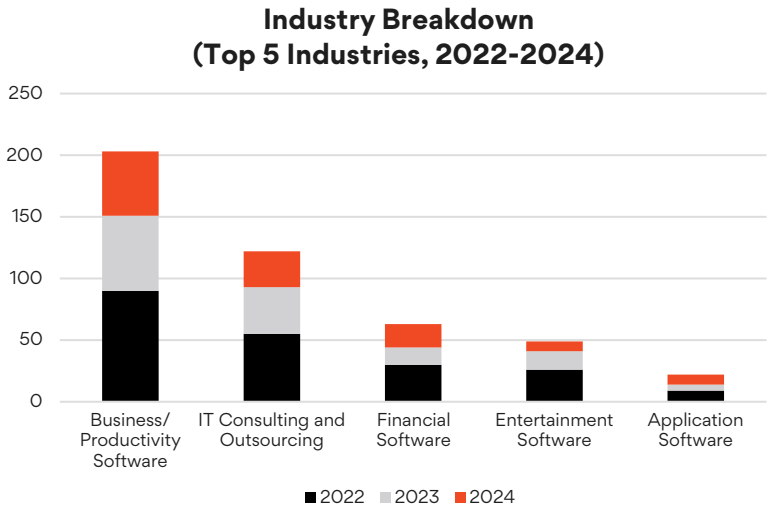
The scope of AI-specific due diligence varies depending on the nature of the target. For instance, if a company provides AI infrastructure or data centres, due diligence may align more closely with standard M&A considerations, with some exceptions, such as ensuring sufficient power generation capabilities or access to specialized chips. Conversely, conducting due diligence on machine learning and generative AI providers may require a more bespoke approach to better understand the unique characteristics and risks of the company and its technology. This may include targeted inquiries into personnel and AI systems to evaluate critical areas such as data integrity, model robustness, ethical design processes, and the expertise of specialized personnel.

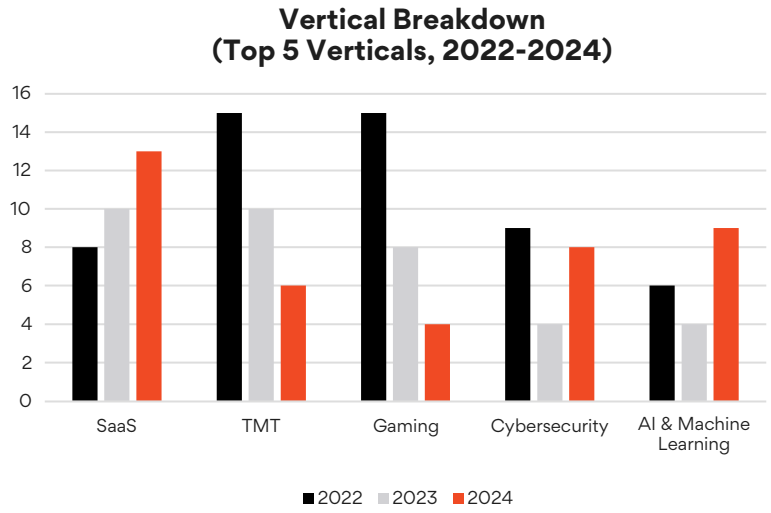
Representations, Warranties and Covenants

M&A transactions involving AI technologies often include representations and warranties typical of Tech M&A transactions, particularly those related to intellectual property rights, data privacy, and cybersecurity. However, recent acquirers are increasingly seeking AI-specific representations, especially when a target's valuation hinges on a specific aspect of this technology or when addressing the unique risks posed by unsettled law. Some representation and warranty insurers are also placing special attention on the qualifications and expertise of those assessing AI technologies and requiring deliberate consideration in the due diligence process. As more companies move to include AI-specific representations and warranties, we can foresee a similar rise in insurers implementing this practice or developing policies with AI-specific coverage and exclusions.

In situations where the law on AI technology remains unsettled—such as with generative AI or the use of web-scraped data—standard representations may not be sufficient. Acquirers might require specific representations to ensure that AI models were trained using permissioned data or that the AI systems align with the acquirer's risk tolerance concerning bias, explainability, and trustworthiness. They may also negotiate specific indemnities and other unique deal terms, such as AI-specific covenants that prohibit changes to a target's training data or AI vendors, models, or compliance policies between signing and closing to maintain the value of the business or asset. Conversely, targets may seek representation and warranty insurance or look to include carve-outs within representations and warranties to avoid a breach due to changes in the law that are outside of their control.

Ultimately, the unique risks associated with AI necessitate tailored due diligence, representations and warranties and covenants to adequately protect against and manage uncertainties in Tech M&A transactions.





Trend #2: Market dynamics will shift vendor pricing and customer opportunities for cost-savings

DYNAMICS SUPPORTING VENDOR PRICE INCREASES

As customers will recognize, certain changes in the market have led to increasing pressure from technology vendors to raise prices. For example:

1. **M&A Acquisitions have led to Increased Pressure on Vendors to Deliver Financial Returns**: The technology sector has seen a significant uptick in M&A activity, particularly driven by private equity firms buying technology companies to create synergies, consolidate market positions, and ultimately drive higher margins (e.g. the Broadcom acquisition of VMware at the end of 2023). Newly acquired firms often face substantial pressure to deliver improved financial returns, contributing to across-the-board price hikes.

2. **Changes in Vendor Pricing Models**: Technology vendors are redefining how they price their products. For example, on the licensing side, Oracle recently made the decision to price Java based on the number of *employees* rather than the number of *licenses*.

3. **Transition to Subscription-Based Licence Models**: In a similar vein, there continues to be a marked movement by vendors from a perpetual license model to a subscription-based, and recurring payment, Software as a Service (SaaS) model. For example, (a) Guidewire, a technology vendor for the P&C insurance industry, recently transitioned from an on-premises (on-prem) license model to a SaaS model, and (b) in 2025, IBM is migrating key products such as Maximo and Cognos from perpetual licensing to SaaS. All of this is part of a broader strategy to move customers into recurring payment models. Not only do such vendor-hosted models raise new customer concerns regarding vendor security and data breach obligations, but each expiration of a subscription term becomes a further opportunity for vendors to implement price increases.

4. **Accelerated End of Life (EOL) Cycles**: Vendors are accelerating the discontinuation of support for older software versions, effectively forcing customers to upgrade at higher costs. Under the previously dominant on-prem licensing model, software vendors had heavily relied on the maintenance support fees (which could be 20% or more of the license cost) as an ongoing annuity revenue stream. With the on-prem licensing model going the way of the dodo, vendors have sped up the EOL cycle - for among other reasons, to maintain revenue by incenting customers to purchase the upgraded successor versions.

5. **Increased Compliance Audits**: Suppliers are conducting rigorous audits to uncover instances of licence non-compliance. These audits can lead to unexpected costs and necessitate additional investments in compliance measures. For example, the IBM audit practices remain aggressive. In 2025, IBM is expected to not only audit any customer not audited in the last four years, but also to enforce mandatory verifications – effectively audits in all but name - at the end of the term of each of their Enterprise License Agreements. Similarly, Oracle is expected to intensify its customer licence audit activity throughout 2025, having recognized audits as a critical revenue stream, with particularly increased scrutiny of OCI Cloud, Oracle Java, and on-prem software licenses.

DYNAMICS COUNTERING VENDOR PRICE INCREASES

Yet there are other dynamics at play which are countering these trends. Market uncertainties have resulted in a slowdown in the availability of RFPs/RFIs on which vendors can bid, so customers have reported that, in some cases, vendors have quickly compromised in response to customer pushback on vendor-requested price increases - based on the vendor rationale that it is better to keep some market share than to lose market share in a push for fee increases. In other sectors, plateauing revenues for customers – for example, in the insurance industry – have heightened the focus on cost-cutting, creating another dynamic to counter the technology vendor push for increased fees.

However, the ability of a customer to resist price increases depends on the materiality of the software to the customer. For example, it is easier to pivot – or to threaten to pivot – to a cheaper alternative vendor where the applicable product is more of a utility; it becomes much less of an option where the product is part of a very large and/or complex Enterprise Resource Planning (ERP) implementation.

Customers can seek to improve their ability to pivot from, and therefore negotiate better pricing with, each vendor, by implementing proactive strategies such as (a) obsolescence analysis/EOL forecasting of their technology inventory, in order to identify in advance components for which EOL is pending, and (b) adopting a “second sourcing” strategy, wherein the customer identifies and engages an alternative, secondary vendor as a backup to the primary vendor, ensuring that the customer is not solely dependent on a single vendor.

THE CONTINUING ISSUES POSED BY TIME & MATERIAL ENGAGEMENTS

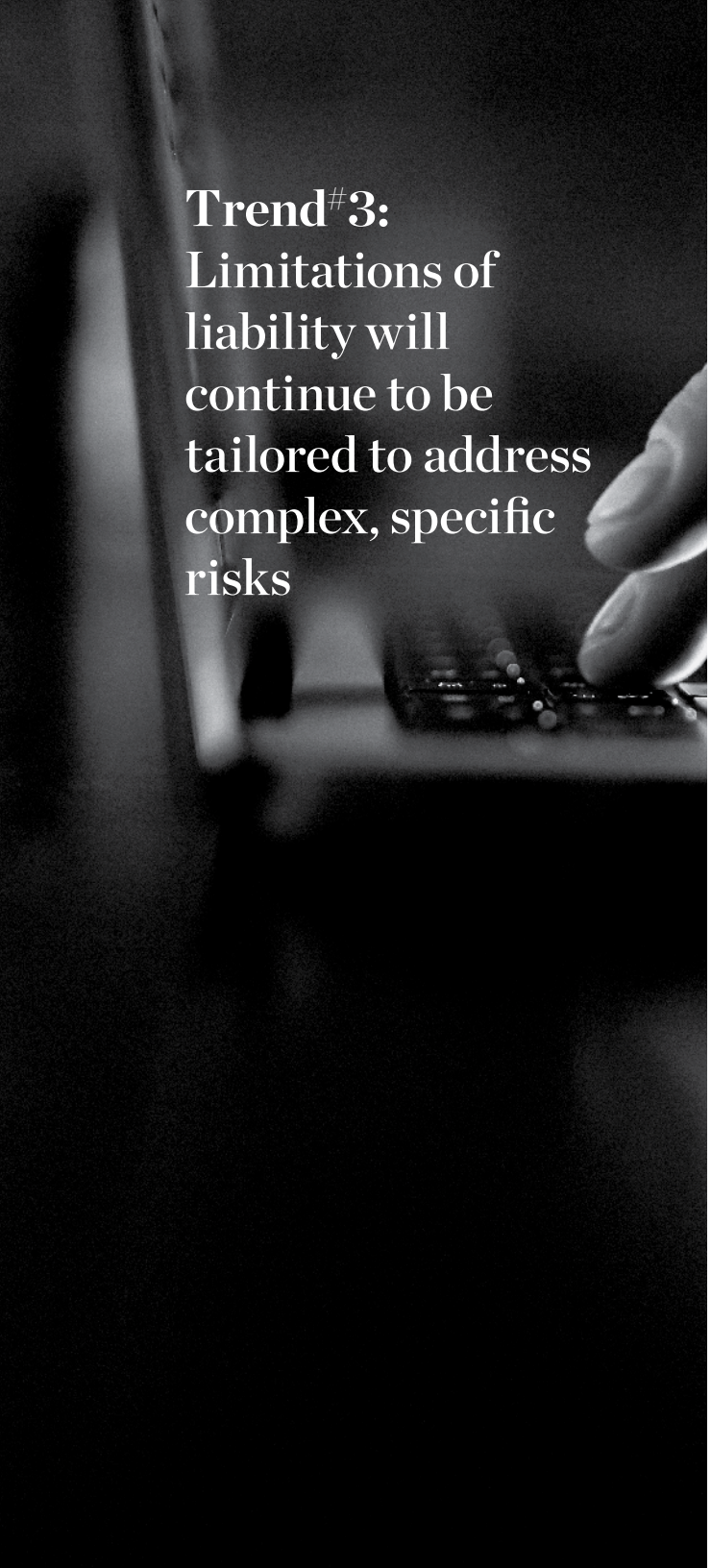
As a final comment, failed project lawsuits continue to suggest that there can be an over-reliance on time and material (T&M) engagements in the ERP and technology project space, which can present challenges. As one example only, in *Hertz Corporation v Accenture LLP*, 1:19-cv-03508 (SD NY 2019), the customer learned this to their detriment when they engaged the vendor to complete a digital channels engagement on a T&M basis, but after paying the vendor more than US$32 million in fees and expenses, argued that they never received a functional website or mobile app.

Customers should be very careful in considering whether to agree to T&M fee structures for large scale technology projects. In some cases, customers – knowing that contingency is built into a fixed fee price - may think that they are 'outgaming' the vendor by agreeing to a T&M engagement which avoids the contingency amount. However, this will not necessarily be the case, and can present a fundamental challenge.

From the customer perspective, a fixed fee engagement has the advantage of a more defined list of vendor justifications where a project encounters cost overruns: for example, the vendor might justify the cost overruns based on a failure of the customer to perform their obligations, or on customer scope creep. In contrast, in a T&M engagement, the vendor does not need to reference such a list of justifications, as fee expenditures are simply based on time spent.

For the customer, a second advantage of a fixed fee project is that it requires the vendor to put "skin in the game". The customer's position will be that, if a vendor is claiming to have extensive experience and expertise with respect to the technology project, then they should be able to emerge a fixed fee to accomplish such project. The vendor can still protect themselves with a crisply defined scope and a built-in contingency amount, and by enumerating specific assumptions and customer obligations in order to qualify that fixed fee, but on the whole, the fixed fee could still more fairly allocate the project risk.

From the vendor perspective, a T&M engagement may be preferable in various circumstances, including for engagements of limited scope, but with a high degree of uncertainty. For example, T&M might be more suited (a) for the initial planning phase of a project, rather than for the "build" phase, (b) for an initial due diligence "Phase 0" for a project, or (c) for a multi-vendor project where the success of the vendor will be reliant on the performance of other third party contractors outside the control of the vendor. We expect to see a continuing push by vendors for T&M engagements where the vendor faces inadequate information, or a lack of control over externalities on which the success of the project may be reliant.



Trend#3: Limitations of liability will continue to be tailored to address complex, specific risks

Limitation of Liability (LoL) clauses are a cornerstone of IT agreements, designed to allocate risk between contracting parties and cap potential liabilities. As technology continues to evolve and the scope of IT services expands, these clauses have become increasingly complex and tailored to address specific risks. This section examines recent trends in LoL clauses across various IT agreements, focusing on liability caps, the scope of exclusions, and specific LoL clauses.

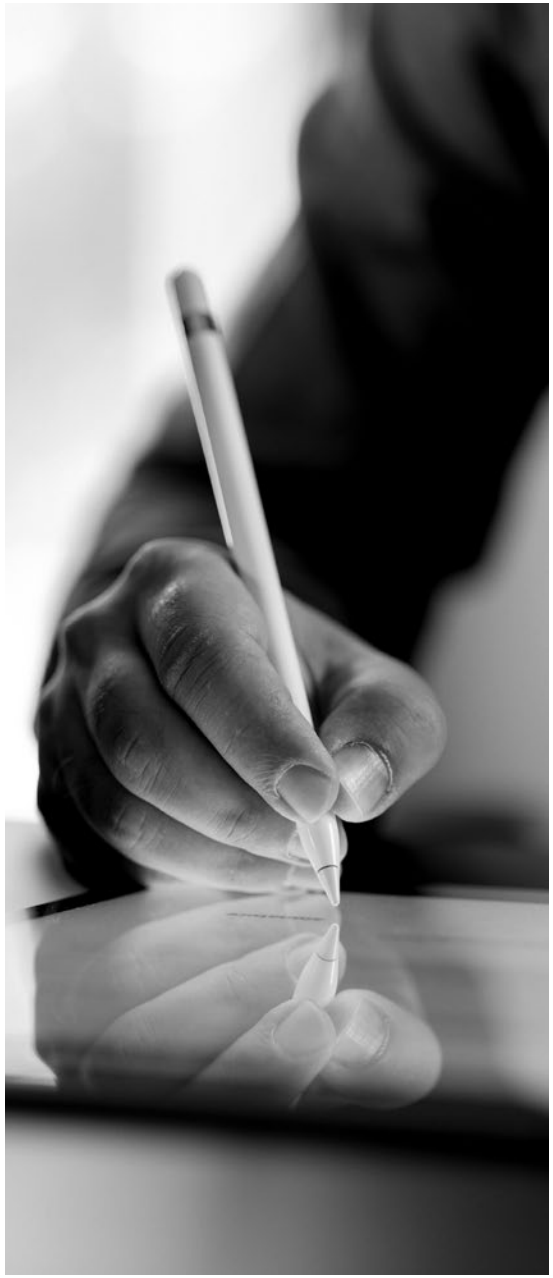
LIABILITY CAPS

In 2024, caps and supercaps continued to take various structures, with the most common being based on the value of the contract or a multiple of the fees paid over a specified period. For instance, some agreements capped liability at the total fees received for the product or service, while others set caps at a negotiated amount, which bore connection to the total value of the contract, with annual adjustments. 2024 saw increased attention on cost of living adjustments (COLA) in light of inflation concerns and rising interest rates, which may taper slightly this year as the Bank of Canada predicts reduced inflation for 2025 and has since been cutting interest rates.[2]

The use of cap reset mechanisms also gained traction in the market. These mechanisms effectively reset the liability cap to its original quantum in the event of specific breaches, or where the payment of damages exceeds a particular threshold (50%) within a specific period of time (12-36 months).

For 2025, we expect that these clauses will continue to take on a variety of structures and quantums, reflecting the nuances in the particular nature of the relevant IT services and the varying levels of risk associated with different types of agreements.

2. https://www.bankofcanada.ca/publications/mpr/mpr-2024-10-23/projections/; https://capitalmarkets.bmo.com/en/news-insights/markets-plus/2025-canada-economic-outlook-on-the-mend/



EXCLUSIONS FROM LIABILITY

Another key element in LoL clauses is the exclusion from liability for certain types of damages. Liability exclusions for indirect, consequential, exemplary, punitive, and special damages continued to be a common practice in 2024. Lost profits, business interruption, and loss of data were likewise common exclusions; however, there were notable variations in how they were applied. In certain cases, consequential damages may be an appropriate remedy and, therefore, were not subject to the exclusion from liability. Certain agreements provided exceptions for specific types of breaches or indemnity obligations, ensuring that certain critical risks were not subject to the exclusion from liability. For example, breaches of confidentiality, privacy, and security obligations were often carved out from these exclusions, reflecting the heightened importance of these issues within the IT industry, particularly with the advent of artificial intelligence and the increased prevalence and financial risk of data breaches. We expect these trends to continue into 2025.

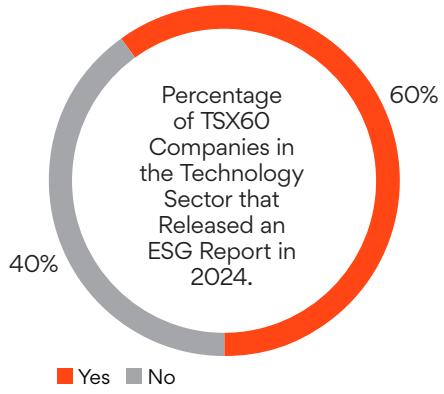
SPECIFIC LIMITATION OF LIABILITY CLAUSES

In addition to the more traditional elements of LoL clauses, IT agreements often include distinct provisions that are tailored to address specific IT operational risks. One such provision is the concept of deemed direct damages, which could apply to scenarios where certain failures result in specified financial losses. For example, deemed direct damages may be included for revenue losses resulting from system failures or other disruptions. Similarly, some agreements include expenses for retaining strategic third-parties to respond to or advise on events or breaches such as those involving personal information, confidentiality, or security obligations. With several notable IT disruptions in 2024, we anticipate these provisions will remain highly relevant in 2025. Certain IT services are critical and parties will likely seek to ensure that they are compensated for specific types of losses that might otherwise be excluded under traditional limitation of liability provisions.

Trend #4: The ESG regulatory landscape will continue to evolve and find both support and challenges from technology innovation

Environmental, Social, and Governance (ESG) factors remain central to corporate strategies across Canada, driven by both global sustainability concerns and increasing regulatory pressures. In Canada, ESG practices are becoming increasingly formalized, with significant changes in the regulatory landscape over the past year. The *Fighting Against Forced Labour and Child Labour in Supply Chains Act*, which came into effect on January 1, 2024, mandates companies to disclose efforts to eliminate forced and child labour in their supply chains.[3] Failure to comply with these new regulations could result in penalties of up to CAD $250,000 for non-compliant entities, officers, or directors.[4]

Further, amendments to the Canadian *Competition Act*, effective since June 2024, explicitly prohibit greenwashing and require that environmental claims made by companies be substantiated by proper testing and globally accepted standards.[5] This legislation will further impact how tech companies disclose their environmental initiatives. Simultaneously, the growing anti-ESG sentiment, particularly in the United States, is influencing the broader business environment, creating political sensitivities that organizations must navigate carefully.[6] To remain competitive and compliant, technology firms need to stay updated on both regulatory changes and shifting public attitudes toward ESG, ensuring they can balance the demands for transparency with the potential challenges posed by opposing movements.



3. ***Fighting Against Forced Labour and Child Labour in Supply Chains Act*** (S.C. 2023, c. 9)
4. Ibid. at 19(1)
5. https://competition-bureau.canada.ca/how-we-foster-competition/education-and-outreach/environmental-claims-and-greenwashing
6. https://www.thomsonreuters.com/en-us/posts/esg/anti-esg-legislation/

AI AND INNOVATION: OPPORTUNITIES AND CHALLENGES GOING FORWARD

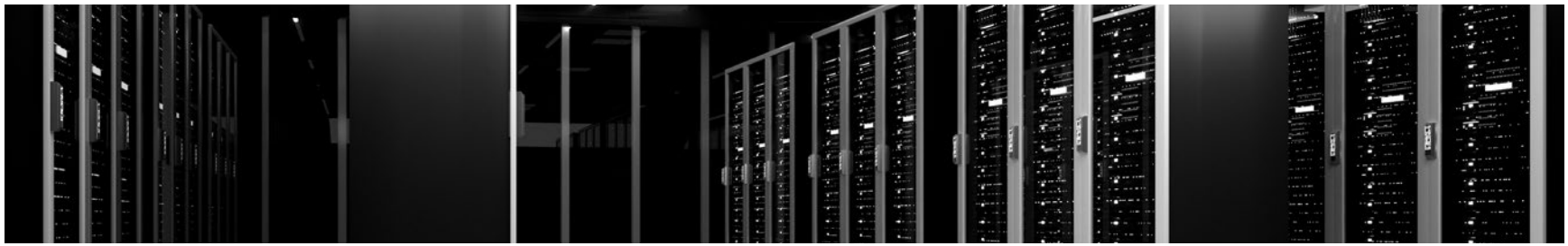
Artificial intelligence is increasingly a key focus in ESG discussions as companies and investors acknowledge its growing influence. From an ESG perspective, AI offers opportunities to enhance transparency and efficiency, particularly in tracking, analyzing, and comparing ESG data. However, AI also introduces new challenges, including privacy risks, algorithmic biases, and the environmental impacts of large-scale AI systems.

One major challenge is the increasing demand for data centers driven by AI, which consume vast amounts of energy and water. For example, the electricity consumed by an AI chatbot, such as ChatGPT, can be up to ten times greater than a typical Google search. The International Energy Agency estimates that electricity consumption from data centers and AI could exceed 1,000 TWh by 2026, roughly equivalent to the total electricity consumption of Japan.[7]

However, advancements in data center infrastructure have made significant progress in reducing energy demands. The rise of green data centres, which prioritize energy efficiency and sustainability, plays a key role in this. These facilities employ technologies such as efficient cooling systems, renewable energy sources, and waste heat reuse to optimize energy use. In addition, innovations such as AI model optimization and energy-efficient hardware further help minimize AI's carbon footprint. Going forward, it will be important to see how nations, including Canada, balance these technological advancements with regulatory measures to manage the explosion in energy demand.

On the governance and social fronts, investors are increasingly concerned about AI risks and pushing for responsible AI governance frameworks. This has led to a rise in shareholder proposals, especially in the United States, urging companies to disclose AI usage, establish ethical guidelines, and ensure adequate board oversight. As AI adoption spreads across industries, tech companies must address both regulatory requirements and growing investor demands for transparency and ethical AI practices. Organizations that proactively manage these risks and demonstrate responsible AI use are more likely to earn investor trust and maintain a competitive edge.

Ultimately, the ESG landscape in Canada is rapidly evolving, with new regulations and growing investor expectations shaping corporate strategies. For technology companies, staying updated on these regulatory shifts, addressing the challenges posed by AI, and responding to rising concerns around ESG will be critical for long-term success.



7. https://iea.blob.core.windows.net/assets/18f3ed24-4b26-4c83-a3d2-8a1be51c8cc8/Electricity2024-Analysisandforecastto2026.pdf at page 8

Trend #5: Government action will augment the cybersecurity imperative for businesses

The introduction of new federal and provincial cybersecurity requirements represents a significant milestone in the regulation of cybersecurity in Canada. If brought into force in 2025, the federal and provincial legislative amendments and regulations outlined in this section will have a dramatic effect on the security practices of private and public sector organizations, requiring considerable re-evaluation of both internal cybersecurity policies and third-party agreements.

FEDERAL - *BILL C-26, AN ACT RESPECTING CYBER SECURITY, AMENDING THE TELECOMMUNICATIONS ACT AND MAKING CONSEQUENTIAL AMENDMENTS TO OTHER ACTS* (BILL C-26)

As of late December 2024, the federal Parliament was on the verge of passing into law Bill C-26, with the Senate of Canada having completed its Third Reading of the bill and the House of Commons ready to adopt the Senate's amendments and send the legislation for Royal Assent. Bill C-26 nonetheless "died" on the Order Paper following the Prime Minister's decision to prorogue Parliament on January 6, 2025. Bills which have not received Royal Assent before prorogation are terminated and must normally be reintroduced as if they had never existed, though given how far along Parliament was in its consideration of the Bill, it is possible that the same legislation will be reintroduced[8] and swiftly passed into law by a new government (or the next Parliament) in 2025.

If passed into law, the legislation will:

1. Make amendments to the *Telecommunications Act* (including prohibiting the use of products and services of certain suppliers via security orders issued by the Canadian government or the Minister of Industry)
2. Enact the *Critical Cyber Systems Protection Act*, which would apply to certain designated operators of "vital systems and services" (e.g., banking systems, federally-regulated transportation systems, interprovincial power systems). The obligations generally relate to establishing a cybersecurity program, reporting cybersecurity incidents, complying with directions by the Canadian government, and maintaining records related to compliance and incidents

8. Bills can be reinstated at the start of a new session at the same stage they had reached at the end of the previous session. This is accomplished either with the unanimous consent of the House or adoption of a motion to that effect. See: "Effects of Prorogation" https://www.ourcommons.ca/procedure/procedure-and-practice-3/ch_08_6-e.html.

3. Impose significant penalty provisions. For example, the *Critical Cyber Systems Protection Act* will introduce penalties for each type of violation to be defined by the regulations (i.e., minor, serious, or very serious). The penalties for each violation may not exceed $1,000,000 for individuals and $15,000,000 for other persons

Bill C-26 represents a significant assertion of federal jurisdiction into cybersecurity regulation in Canada. In light of the advanced stage that Bill C-26 reached prior to prorogation and the aggressive posture of the incoming US administration towards cybersecurity and national security matters, organizations should be prepared in the event this legislation is resurrected and passed into law in 2025.

ONTARIO - *BILL 194 (STRENGTHENING CYBER SECURITY AND BUILDING TRUST IN THE PUBLIC SECTOR ACT, 2024)*

Bill 194 (*Strengthening CyberSecurity and Building Trust in the Public Sector Act, 2024*) received Royal Assent on November 25, 2024. On a date to be proclaimed, Bill 194 will:

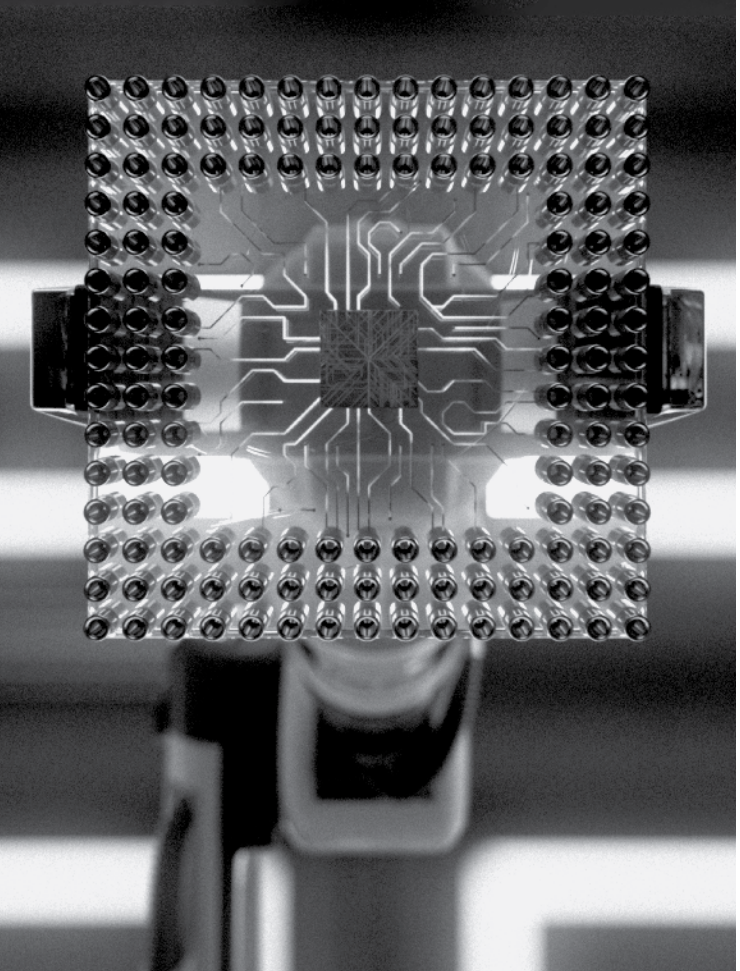
1. Enact the *Enhancing Digital Security and Trust Act*, which allows the Ontario government to require public sector entities to develop and implement cybersecurity programs and submit reports on cybersecurity, among other requirements related to privacy and how public sector entities use AI systems

2. Make amendments to the *Freedom of Information and Protection of Privacy Act* (only part of which came into force on Royal Assent related to "customer service information")

Looking Ahead to 2025

2025 will be a critical year for organizations to assess their cybersecurity programs, including the policies organizations use to protect confidential and personal information. Organizations will also need to review agreements with service providers and assess whether there are sufficient measures in place to ensure compliance with new cybersecurity regulations in Ontario (and, potentially, across Canada). Although public sector institutions are the focal point of Bill 194 in Ontario, private sector organizations should monitor federal and provincial developments closely, keeping a watchful eye on how industry standards shift based on an increasing amount of federal and provincial regulatory oversight of public and private sector cybersecurity.

Trend #6: Customers and service providers alike will increasingly look to insurance to mitigate technology risk



The evolution of digital risk over the course of 2025 will lead more businesses to require their service providers to carry, and those providers will find it prudent to carry, technology errors and omissions (E&O) and cybersecurity insurance. This will be especially true where relevant risks are known or heightened, making it insufficient to rely solely on limitation of liability or indemnification provisions in contracts, particularly where the service providers may be expected to increase efforts to limit their exposure to such known risks. As risk of an event increases, knowledgeable customers often seek to mitigate exposure via insurance (among other means), and knowledgeable providers may seek to reallocate all or part of the risk to their customer.

TECHNOLOGY E&O INSURANCE

Customers will continue to expect that their service providers hold technology E&O insurance and service providers may need to have recourse to such insurance. SaaS companies, in particular, will continue to benefit from technology E&O insurance because they operate in a highly dynamic and competitive environment where the reliability and security of their services is paramount. These companies provide software applications over the public internet or private networks while handling large amounts of data and must ensure relatively uninterrupted access to their services. As a result, SaaS companies and their customers will have a continued focus on technology E&O insurance, in 2025 and the coming years, for at least the following reasons: simple prudence; as a contractual obligation; due to innovation requirements and in response to regulatory compliance obligations.

Prudence by SaaS Providers: Technology E&O insurance use will increase as a means of coping with the increasing complexity of modern digital ecosystems, given its coverage of legal costs and financial liabilities arising from covered risks arising from the storage and processing of sensitive client information, and continuous service availability for SaaS services that are relied on by customers for daily operations.

Expectations for Contractual Obligations: Where SaaS agreements include stringent service level agreements (SLAs) that guarantee specific performance metrics, including uptime and response times, failure to meet these contractual obligations can result in service providers being subject to penalties, refund obligations, and potential legal claims by their customers. Technology E&O insurance helps SaaS companies cover the costs associated with these contractual breaches, providing a safety net that allows them to focus on maintaining high service standards.

Continued Pressures to Innovate and Develop: The SaaS industry is characterized by rapid innovation and continuous development of new features and functionalities. However, the introduction of new technologies and updates may generate additional bugs and other unforeseen

technical issues. Technology E&O insurance provides coverage for claims related to software defects and development errors, enabling SaaS companies to innovate with greater confidence, knowing they have protection against potential liabilities.

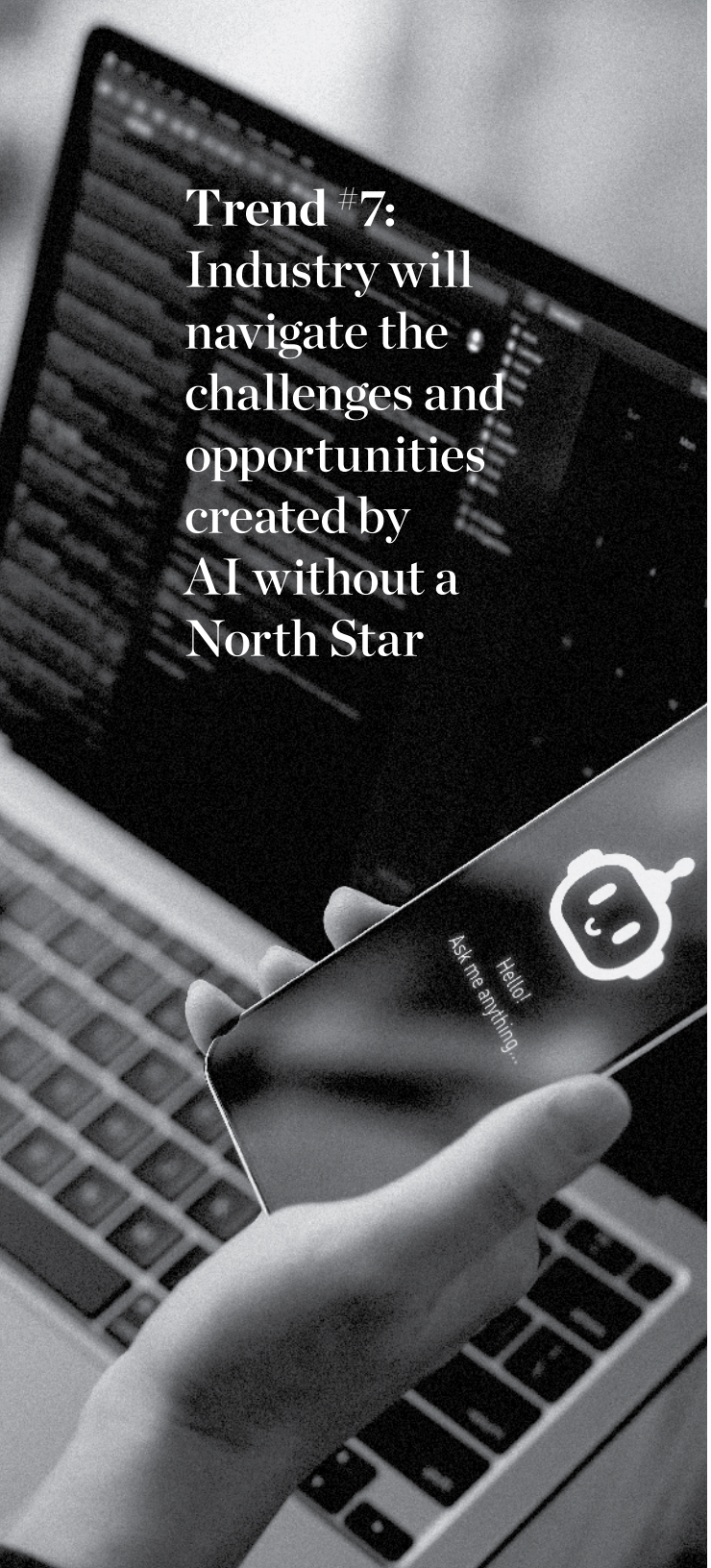
Regulatory Compliance: Non-compliance with data protection and cybersecurity regulations may result in significant fines and protracted and costly litigation. Regulators continue to be attuned to the impact of data breaches, unplanned service outages and general regulatory non-compliance. The risk mitigation that technology E&O insurance offers for legal expenses and penalties related to regulatory breaches will be an increasingly helpful tool to mitigate the risk that comes with navigating a complex regulatory landscape.

CYBERSECURITY INSURANCE

We expect that the trajectory of increasing cyberattacks will continue in 2025, with commensurate shifting of this risk to SaaS providers from customers by contracts requiring SaaS providers to implement comprehensive cybersecurity frameworks, such as regular risk assessments, employee training, and incident response plans. Regulatory compliance will also be a particularly significant factor in 2025, with contracts adapting to meet the stringent requirements of data protection laws and privacy regulatory authorities, especially as new privacy laws and regulations are developed and implemented. We also expect to see a shift toward more tailored policies that continue to address specific industry risks and provide coverage for cyber liability, including incident response, business interruption, and data breach liabilities.

IP INFRINGEMENT INSURANCE

We expect demand for insurance products that protect against IP-related risks, including patent, trademark, and copyright infringement, to grow over the course of 2025. Customers will continue to impose requirements for service providers to obtain insurance coverage to address IP risks, especially where a service provider uses IP owned by third-party subcontractors or where the IP used in outsourced technology service offerings has been the subject of IP infringement litigation (whether domestically or in foreign jurisdiction(s)). Contracting parties may also look to IP infringement insurance to mitigate the risk posed by new technologies, such as artificial intelligence (AI) and machine learning, and the novel IP challenges they introduce. Among the features that both customers and service providers alike may find appealing about IP infringement insurance is its multi-jurisdictional coverage, which helps companies navigate the complexities of global IP enforcement and protection.



Trend #7: Industry will navigate the challenges and opportunities created by AI without a North Star

2024 was generative AI's testing, implementation, and adoption year. Product owners aimed to improve its reliability, address societal implications, build trust, find product-market fit, and make it an essence of daily life, while user organizations outlined use case scenarios that posed reduced risk, focused on policy creation and ethical governance, and training. However, the Canadian legislative framework to regulate AI did not keep up with generative AI's explosive growth and the Canadian government's planned AI-investment of $2.4 billion in 2024. In 2022, the Canadian government tabled the *Artificial Intelligence and Data Act* (AIDA), and amendments were proposed in 2023, after which, AIDA passed the second reading in the House of Commons and was being considered by the House Standing Committee on Industry and Technology. However, with the Canadian Parliament being prorogued in early January, AIDA will die on the Order Paper as a result.

However, the complexity and sophistication of AI systems and an ever-evolving risk landscape, coupled with a lack of a standardized legislative framework, demands that both providers and users of AI systems take proactive measures. Providers need to implement safeguards that make AI systems ethical, reliable and secure. This includes addressing issues of bias, prioritizing fairness and transparency in outcomes, implementing robust security measures, complying with privacy laws, continuous testing to detect vulnerabilities, errors and unintended outcomes, and implementing fixes. On the other hand, users must take pre-emptive de-risking measures. This includes assessing their data infrastructure, compliance with privacy regulations, upskilling and training their workforce, and implementing clear policies and frameworks for responsible use of AI, systems to monitor such use, and mechanisms to address issues promptly.

DATA PRIVACY DEVELOPMENTS

In Canada, despite AIDA's demise, existing federal and provincial privacy laws continue to apply to organizations' use of AI. PIPEDA and provincial laws require that organizations obtain consent for the collection, use, and disclosure of personal information in connection with AI systems and that organizations be accountable for personal information in connection with their use of those systems. You can read our bulletin on a recent Federal Court of Appeal decision on obtaining meaningful consent and the need for organizations to provide specific, direct, and layered notices to individuals so that they can provide informed consent for the collection and use of their personal information. In addition, where AI systems are used to make decisions about individuals, existing privacy laws require that organizations retain personal information so that individuals have a reasonable opportunity to access that information on request. Quebec's revised privacy law also includes specific requirements for decisions made solely on an automated basis by providing individuals with a right to be informed of such decisions and request additional information on how the decision was made.

2025 may also bring the first application of current privacy laws by Canadian privacy regulators to generative AI based on the outcome of the federal, Alberta, British Columbia, and Quebec privacy commissioners' investigation into OpenAI. The privacy commissioners are investigating OpenAI to determine if: (i) it has obtained valid consent for collecting, using, and disclosing personal information via ChatGPT; (ii) it has fulfilled its obligations regarding openness, transparency, access, accuracy, and accountability; and (iii) if the collection, use, and disclosure of personal information are appropriate, reasonable, and legitimate, with a focus on necessary information. The investigation has the potential to consider foundational privacy issues for generative AI, for example whether training is a use of personal information and whether large language models themselves embody personal information. In Europe, a recent European Data Protection Board decision held that training models on data that includes personal data and the resulting models implicate the processing of personal data under the European General Data Protection Regulation. The outcome of the commissioners' investigation could significantly impact how generative AI can be developed, made available, and deployed in Canada.

INTERNATIONAL AI REGULATORY DEVELOPMENTS

Last year, the EU introduced the AI Act, which came into force on August 1, 2024, and whose provisions took effect on February 2, 2025. The EU AI Act classifies AI systems by risk and places restrictions and prohibitions on the various categories of AI systems and uses. You can access our previous bulletin here to know more on the AI Act and the timeline for its application.

In the US, there is currently no comprehensive federal AI legislation. Several bills across a wide range of issues in AI are being considered by the US Congress, with several of them emphasizing the development of voluntary guidelines and best practices for AI systems. In September 2023, the US Senate held public hearings to explore how to increase transparency in AI for consumers, identify uses that are beneficial or "high-risk", and evaluate the potential impact of AI policies designed to increase trustworthiness and US lawmakers simultaneously held closed-door listening sessions with AI developers, technology leaders and civil society groups. Despite there being no federal legislation, various frameworks and guidelines on AI were developed by the Biden administration, though these initiatives were put to rest with the inauguration of President Donald Trump.

INDUSTRY STANDARDS AND OTHER SAFEGUARDS

Prominent industry standards organizations, including the National Institute of Standards and Technology (NIST) and the Industry Organization for Standardization (ISO), have sought to further fill the legislative void by publishing principles and standards that can be voluntarily adopted by organizations that are involved in the design, development, use and evaluation of AI systems. Examples of this include NIST's Artificial Intelligence Risk Management Framework, which aims to equip providers and users of AI systems with approaches that increase the trustworthiness of AI systems and foster the responsible design, development, deployment and use of AI systems, and the ISO/IEC 42001 standard, which provides guidance on how to establish, implement, maintain and continually improve the management of AI systems and address ethical considerations and risks such as traceability, transparency and reliability. Providers that are involved in the development and commercialization of AI systems may adopt some or all of these standards to demonstrate their commitment to responsible AI design and "industry-best" practices. Organizations looking to procure AI systems may require that their providers adhere to these standards in the same manner as they may require adherence to NIST's or ISO's cyber and information security standards.

It is important to note that fundamental legal safeguards continue to apply to the adoption of AI systems. AI-enabled decision-making that is found to be discriminating or otherwise infringes fundamental human rights remains subject to the Canadian Charter of Rights and Freedoms and federal and provincial human rights legislation as it otherwise would be if the decision was made solely by a human. Similarly, federal and provincial consumer protection and employment legislation continue to provide protection to individual consumers and employees, regardless of the extent to which AI systems are utilized by the vendors and employers they engage with.

Trend #8: Governments will impose increasingly stringent rules to protect consumers in the online environment

E-commerce has exploded in popularity over the past five years and has become the primary sales channel for a sizable portion of the marketplace for consumer products and services. Businesses that never sold online started doing so and others who were comfortable in the space began exploring new opportunities such as subscription services. This migration to digital commerce will not slow down anytime soon.

Engaging in e-commerce in Canada means having to navigate a complex thicket of regulatory regimes. Privacy, Canada's anti-spam law (CASL), the federal *Competition Act* and provincial consumer protection laws of general application are just some of the regimes that must be understood when buying or selling through e-commerce. As these laws and regulations are adapted to protect consumers against evolving risks, businesses need to understand what these changes mean for their business and how to ensure compliance without undue burden or cost.

Every business in Canada that sells to consumers must manage compliance with consumer protection law. All provinces and territories have their own consumer protection laws of general application. Organizations must comply with these laws regardless of where they are located; consumer protection laws generally apply to businesses located in Canada but, also, to businesses that supply products or services to consumers in Canada.

As of the start of 2025, both Ontario and New Brunswick have passed updated consumer protection laws that have received Royal Assent but which still have not entered into force. Regardless, these new laws reflect e-commerce-related regulatory trends. A number of the changes that are forthcoming in Ontario pursuant to the new *Consumer Protection Act, 2023* (the New OCPA) are illustrative:

1. **Public Reviews**: under the New OCPA, a concept has been borrowed from Alberta's *Consumer Protection Act*, prohibiting suppliers from preventing consumers from publishing reviews about the supplier or its products. Two provinces have now amended their laws to address practices that may mislead the public through consumer reviews, suggesting there is heightened regulatory sensitivity to transparency around merchants influencing how their products and services are marketed.

2. **Prohibited Terms as Offences**: under current Ontario law, provisions of consumer agreements (including terms of service) that are not enforceable are generally and simply not enforced. The New OCPA, however, goes a step further and provides that the inclusion of prohibited terms in contracts is also considered an offence, potentially exposing businesses to regulatory enforcement actions. This suggests a possible move towards the model already in place in Quebec, whereby provisions that are not enforceable in Quebec are expressly disclaimed. Such a trend reinforces the need for business to be diligent in drafting their e-commerce terms and conditions so as to not introduce unwanted liability.

3. **Contract Amendments**: the New OCPA distinguishes between "continuation" and "amendment" of a consumer contract. The full intent and effect of these concepts is not yet clear but , in early 2025, the Ontario government began a consultation process concerning the content for regulations that will shed light on these concepts. These consultations will generate input on when consumer contracts should require amendment with notice only versus when consent may be required.

4. **Cancellation Methods**: related to the topic of contract amendment is the issue of how consumer contracts can be cancelled. While not an issue expressly addressed in the New OCPA, the aforementioned consultation process raises the possibility of introducing regulations that would help simplify the cancellation process, such as by mandating that contracts have to be cancellable in the same way they were formed (e.g. online contracts have to be cancellable online) or prohibiting business from dissuading consumers from cancelling contracts. Given that similar initiatives are underway in other jurisdictions (most notably a "click to cancel" rule for subscriptions in the USA), such regulation of business processes is a topic for e-commerce providers to keep an eye on.

The modernization of Ontario's consumer protection regime illustrates how business must continually adapt to the laws governing e-commerce. As Ontario and other Canadian jurisdictions continue to evolve their consumer protection laws, businesses would benefit from legal advice regarding how to navigate this new landscape successfully.

Trend #9: Innovation in fintech will continue and adoption will increase despite ongoing challenges

Financial technology (fintech) products are innovating rapidly to meet the expectations of consumers for convenient and cost-effective services to facilitate digital payments, investments, capital raising, and other digital financial services. Despite recent growth, the fintech sector in Canada continues to lag behind some other G7 countries in terms of adoption and market size. In 2023, only 13% of Canadian banking consumers were found to use fintech services, compared to 32% in the United Kingdom and 42% in the United States.[9] Momentum is on an upward trajectory, however, with data showing that Canadians in 2023 were three times more willing to share data with financial service providers that they have an existing relationship, as compared to 2020.[10] We expect this trend has continued in 2024 and will also be seen in 2025. Regulatory developments are likely to play a significant role in the growth of the fintech sector in Canada, as they have in the UK and the US.

OPEN BANKING IN CANADA

Open banking, or consumer-driven banking, is a framework that allows users to provide third-party service providers access to a consumer's bank account data. Traditionally, banks have kept customer financial data within their own closed systems. Open banking allows consumers to safely share their financial information with fintech companies, widening access to financial services such as money transfers, aggregated account management, and personalized financial insights.

To utilize innovative fintech services, established financial institutions have been turning to strategic acquisitions of fintech companies or partnerships with fintech companies to improve customer experience for their own platforms. We expect this trend to continue.

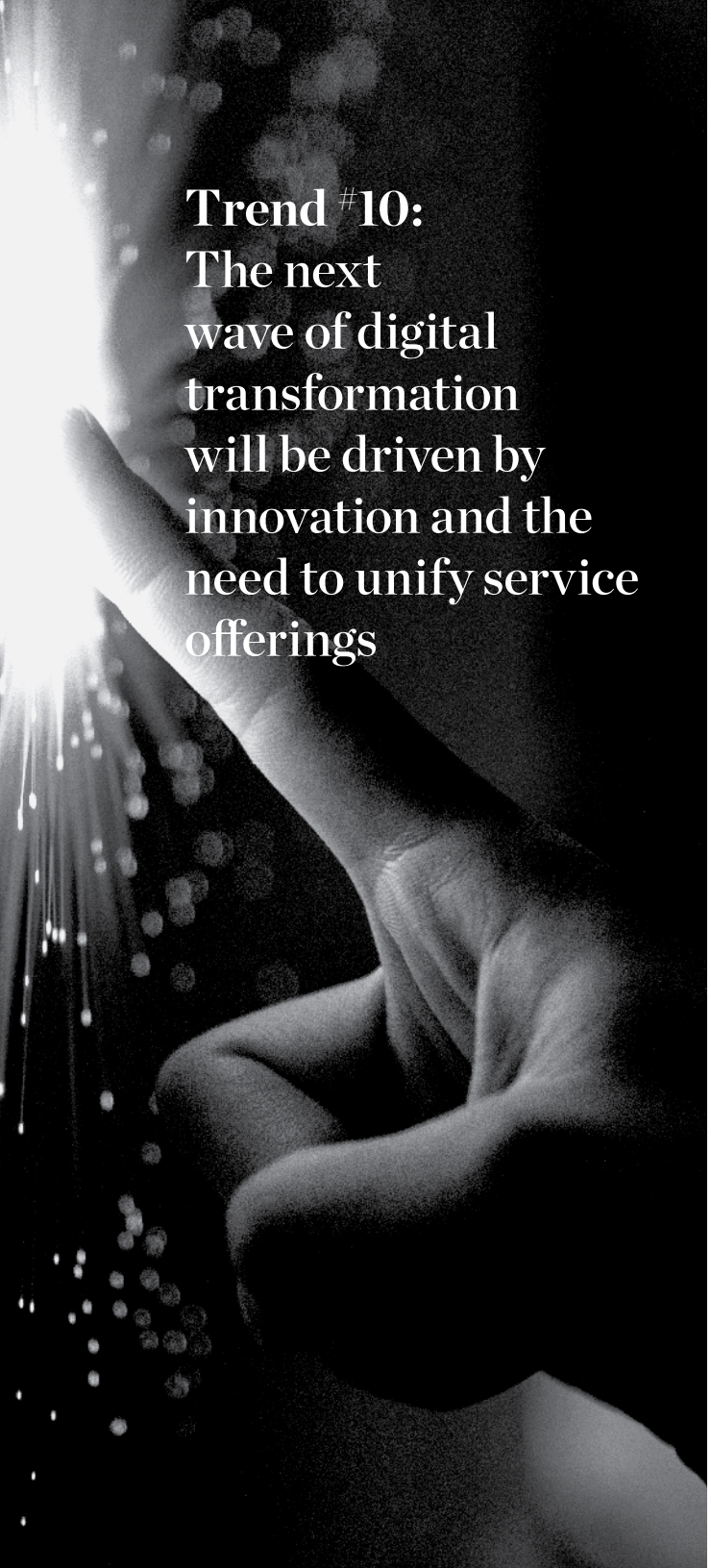
9. Fintech companies in Canada: Is the industry ready to boom? | McKinsey
10. Canadians are 3x more likely to share data with their financial service providers today than 2020, finds EY survey | EY - Canada. See also ca-open-banking-in-Canada-improving-awareness-transparency-and-trust-aoda.pdf (SECURED).

However, the majority of fintech companies are unable to securely access customer information from established financial institutions because Canada lacks requirements compelling them to do so. As a result, fintech companies must resort to using a practice known as "screen scraping" wherein the customer provides the fintech company their bank credentials so the company can log into the customer's bank account intermittently to access their financial information. This practice carries significant security and liability risks in the event of unauthorized transactions or data breaches. Leaders in the fintech sector have publicly voiced their concerns over Canada's slow rollout of open banking legislation compared to other advanced economies. On the other hand, established financial institutions have raised fundamental concerns regarding the regulation, or lack thereof, of fintech companies as well as concerns about high compliance costs.

In April 2024, the federal government announced that it was developing a framework for open banking in the federal budget and allocated more than $5 million for this initiative over the next three years. In June, the *Consumer-Driven Banking Act* was passed.[11] This legislation expands the mandate of the Financial Consumer Agency of Canada to include oversight of a new Consumer-Driven Banking Framework. The federal government's Fall Economic Statement from December 2024 announced that the framework is set to launch in early 2026, with an increased implementation budget of $44.3 million over three years, beginning in 2025-26.[12]

Political priorities can change and a new federal government in 2025 may direct its energy to other initiatives in the financial sector, but we expect to see continued innovation and growth in the fintech sector in 2025, with pro-consumer partnerships between fintech companies and financial institutions continuing to play a significant role.

11. Budget 2024
12. 2024 Fall Economic Statement



Trend #10: The next wave of digital transformation will be driven by innovation and the need to unify service offerings

The accelerating pace of digital transformation in 2025 will be characterized by several key trends, with organizations investing in platform unification and leveraging technologies such as AI, cloud computing, and low-code platforms to automate processes, bolster user experiences, unlock efficiencies and innovation, and empower their workforce.

PLATFORM UNIFICATION: BRINGING IT ALL TOGETHER FOR ENDLESS POSSIBILITIES

A central pillar in digital transformation, platform unification simplifies complex IT ecosystems, enhances operational efficiency and agility, reduces fragmentation and costs, and enables better management and decision-making. Below are some of the key areas where unification is surging and will continue to surge:

- Unified ERP and CRM Systems are increasingly becoming the norm for streamlining operations, customer interactions, and enterprise resource management. These systems allow for data consolidation across departments, elimination of redundancies, and provide a holistic view of both internal operations and customer interactions, fostering improved efficiency, collaboration, and decision-making.

- Software and API unification addresses the growing needs for interoperability across contrasting systems (such as legacy and newer systems). API unification reduces integration complexity, accelerates development cycles, and enhance scalability. As organizations adopt hybrid and multi-cloud environments, unified APIs enable flexibility and portability, ensuring that applications can adapt to evolving technologies and regulatory requirements without significant rework.

- Cloud Architecture will evolve due to a steep surge in the Hybrid and Multi-Cloud solutions using Cloud Management Platforms. Gartner predicts end-user spending on cloud services to grow from US $595.7 billion in 2024 to a staggering US $723.4 billion in 2025 - a 21.5% increase. Hybrid and multi-cloud solutions distribute risk by reducing reliance on single vendors, enable AI and machine learning at scale, and increase cloud resilience from cyber threat actors. Supercloud, a unified management layer, will bring simplicity, harmony and control to the chaos of hybrid environments and deliver seamless data access and governance across on-premises, public, and private clouds.

Table 1. Worldwide Public Cloud Services End-User Spending Forecast (Millions of US Dollars)

	2023 Spending ($)	2023 Growth (%)	2024 Spending ($)	2024 Growth (%)	2025 Spending ($)	2025 Growth (%)
Cloud Application Infrastructure Services (PaaS)	142,934	19.5	172,449	20.6	211,589	22.7
Cloud Application Services (SaaS)	205,998	18.1	247,203	20.0	295,083	19.4
Cloud Business Process Services (BPaaS)	66,162	7.5	72,675	9.8	82,262	13.2
Cloud Desktop-as-a-Service (DaaS)	2,708	11.4	3,062	13.1	3,437	12.3
Cloud System Infrastructure Services (IaaS)	143,302	19.1	180,044	25.6	232,391	29.1
Total Market	**561,104**	**17.3**	**675,433**	**20.4**	**824,763**	**22.1**

Note: Totals may not add up due to rounding.

Source: Gartner (May 2024)

AI AUTOMATION: UNLOCKING NEW EFFICIENCIES

Operationalization of Generative AI: The operationalization of generative AI will remain a gradual process in 2025, particularly for organizations in regulated industries, as they grapple with the challenges of integrating this transformative technology. While large language models and other generative tools hold significant potential for streamlining document drafting, automating customer service, and enhancing creative workflows, many enterprises have yet to fully realize these efficiency gains. Legal and compliance hurdles—such as concerns over intellectual property rights, liability for AI-generated errors, and adherence to privacy regulations—remain key concerns for organizations.

AI Agents (The Killer App?): Autonomous AI agents capable of managing workflows, making decisions, and learning from interactions are gaining traction in fields like logistics, finance, and customer relations, to name only a few. However, their deployment within organizations presents key legal risks and challenges, including accountability for errors or harmful outcomes of AI systems, data privacy compliance, potential bias in decision-making processes, intellectual property issues, and ensuring adherence to applicable regulations and standards.

Data Governance: Ensuring Quality and Compliance: The rise of AI applications highlights the need for strong data governance to ensure compliance and make the most of these technologies. High-quality data is essential, as inaccurate or inconsistent data can lead to poor results and reduced trust in AI-generated content. Organizations using AI-driven tools must navigate changing privacy laws while ensuring their data is accurate and reliable, for example, by executing appropriate data-sharing agreements, implementing proper record-keeping practices, and integrating privacy considerations into their use and adoption of AI systems to ensure compliance and obtain the best return on their investment.

WIDER ADOPTION OF LOW-CODE/NO-CODE PLATFORMS

Platforms such as Microsoft PowerApps, OutSystems, Appian, Mendix, and others are empowering non-technical staff to build and deploy applications quickly, significantly reducing development timelines. While these tools democratize innovation, they also raise concerns around security, compliance, and intellectual property ownership. 2025 will require legal teams to guide organizations carefully in implementing usage policies and securing robust licensing and services agreements.

Contacts

Fasken's Technology group is a recognized leader and one of the largest and longest-tenured technology law teams in Canada. Our national team has built a legacy of resolving our clients' most challenging IT issues. We have extensive experience acting for technology providers and users in connection with the development, protection, and commercialization of technology products and services, and assisting buyers and sellers with the acquisition and disposition of technology businesses.

We advise on everything from complex commercial IT transactions, including large systems implementations, outsourcing arrangements, and XaaS arrangements, to internet business models, e-commerce, new technologies (such as quantum computing, artificial intelligence, and blockchain), technology acquisitions/divestitures, and data protection.

Our team is here to help you achieve your business goals. For more information or to discuss a particular matter, please contact us.

Andrew S. Nunes
Partner | Toronto
+1 416 865 4510
anunes@fasken.com

Andrew C. Alleyne
Partner | Toronto
+1 416 868 3338
aalleyne@fasken.com

John Beardwood
Partner | Toronto
+1 416 868 3490
jbeardwood@fasken.com

Daniel Fabiano
Partner | Toronto
+1 416 868 3364
dfabiano@fasken.com

Gabriel M.A. Stern
Partner | Toronto
+1 416 865 5494
gstern@fasken.com

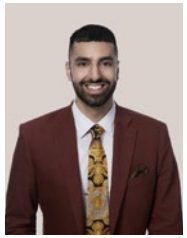
Christopher Ferguson
Partner | Toronto
+1 416 865 4425
cferguson@fasken.com

Ariel Laver
Partner | Vancouver
+1 604 631 3201
alaver@fasken.com

Karam Bayrakal
Partner | Vancouver
+1 604 631 4850
kbayrakal@fasken.com

Jocelyn Auger
Partner | Montréal
+1 514 397 7694
jauger@fasken.com

Paul Burbank
Associate | Toronto
+1 416 865 4427
pburbank@fasken.com



Shan L. M. Arora
Associate | Toronto
+1 416 865 5412
sarora@fasken.com

Anagha Nandakumaran
Associate | Toronto
+1 416 865 5412
anandakumaran@fasken.com

Summer Lewis
Associate | Toronto
+1 416 865 5490
slewis@fasken.com

Julie He
Associate | Toronto
+1 416 865 5407
jhe@fasken.com

Keihgan Blackmore
Associate | Toronto
+1 416 868 7870
kblackmore@fasken.com

Aniket Bhatt
Associate | Toronto
+1 416 868 7871
abhatt@fasken.com

Hannah Im
Articling Student | Toronto
+1 416 865 5439
him@fasken.com

Dongwoo Kim
Articling Student | Toronto
+1 416 865 5168
dwkim@fasken.com

FASKEN

Own tomorrow

About the Firm

As a premier law firm with over 950 lawyers worldwide, Fasken is where excellence meets expertise.

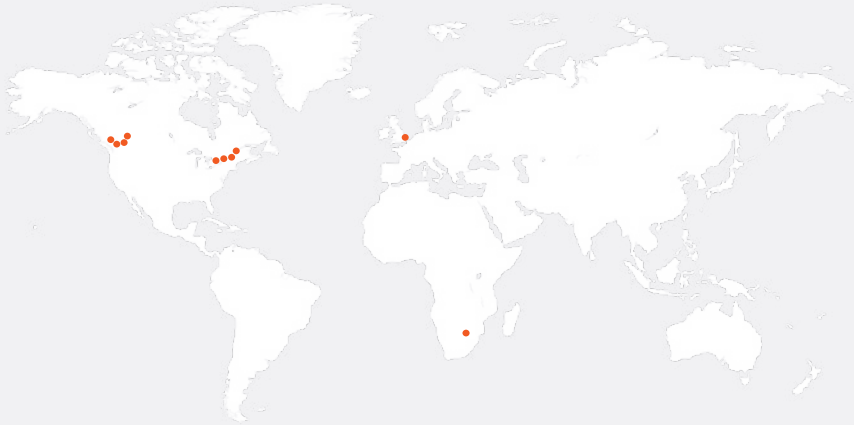
With 10 offices in Canada, the United Kingdom and South Africa, we work to solve complex issues across a wide range of industries and practice areas.

We are dedicated to shaping the future our clients want, precisely when it matters most.

fasken.com

As a premier law firm with over 950 lawyers worldwide, Fasken is where excellence meets expertise. We are dedicated to shaping the future our clients want, precisely when it matters most.

For more information, visit fasken.com.



VANCOUVER	550 Burrard Street, Suite 2900	+1 604 631 3131	vancouver@fasken.com
SURREY	13401 - 108th Avenue, Suite 1800	+1 604 631 3131	surrey@fasken.com
TSUUT'INA	11501 Buffalo Run Boulevard, Suite 211	+1 587 233 4113	tsuutina@fasken.com
CALGARY	350 7th Avenue SW, Suite 3400	+1 403 261 5350	calgary@fasken.com
TORONTO	333 Bay Street, Suite 2400	+1 416 366 8381	toronto@fasken.com
OTTAWA	55 Metcalfe Street, Suite 1300	+1 613 236 3882	ottawa@fasken.com
MONTRÉAL	800 Victoria Square, Suite 3500	+1 514 397 7400	montreal@fasken.com
QUÉBEC	365 Abraham-Martin Street, Suite 600	+1 418 640 2000	quebec@fasken.com
LONDON	6th Floor, 100 Liverpool Street	+44 20 7917 8500	london@fasken.com
JOHANNESBURG	Inanda Greens, 54 Wierda Road West, Sandton 2196	+27 11 586 6000	johannesburg@fasken.com

FASKEN

Own tomorrow

fasken.com