ADVERTISING SUPPLEMENT

IAN C. BALLON, PERVEZ DELAWALLA AND ADAM TELANOFF SHARE INSIGHTS ON WHAT BUSINESSES NEED TO KNOW IN THE AGE OF AI

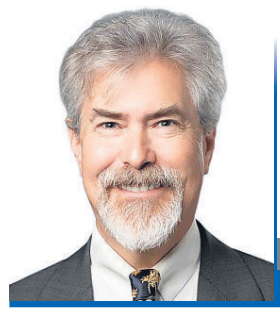
The **Age of AI** roundtable discussion is produced by the LA Times Studios team in conjunction with Greenberg Traurig, LLP, Parker Shaffie, LLP and VegaNext.



Ian C. **BALLON**
Co-Chair, Global Intellectual Property & Technology Practice Group
Greenberg Traurig, LLP
ballon@gtlaw.com
gtlaw.com



Pervez **DELAWALLA**
Chief Executive Officer
VegaNext
pervez@veganext.com
veganext.com



Adam **TELANOFF**
Senior Counsel
Parker Shaffie, LLP
telanoff@parkershaffiellp.com
parkershaffiellp.com

Artificial intelligence is reshaping the way organizations operate, innovate, and compete across virtually every industry. From automating routine tasks to unlocking new insights through data, AI is driving a profound shift in how businesses think about productivity and decision-making.

In this roundtable discussion, three leading experts on the topic share their perspectives on the current state of AI, emerging trends and practical strategies for successful implementation. They explore how companies can balance innovation with responsibility, integrate AI tools effectively into their workflows and address workforce concerns as automation accelerates.

Whether you're in finance, healthcare, manufacturing or professional services, their insights shed light on how AI is transforming business models and redefining the skills needed to thrive in a digital-first future. Join us as we unpack the promise, challenges and next frontiers of artificial intelligence in today's dynamic business environment.

Q: WHAT ARE THE MOST SIGNIFICANT TRENDS IN AI THAT BUSINESSES SHOULD BE PAYING ATTENTION TO AS WE HEAD TOWARDS THE END OF 2026?

A: BALLON:

The most significant trend this year has been the move from generative AI to agentic AI. AI has been – and continues to be – a powerful tool for businesses and individuals. But increasingly businesses are programming AI agents to act autonomously based on prescribed directions or semi-autonomously, subject to human approval. As an AI lawyer, this has introduced a host of new legal issues for companies to consider to mitigate their risk of exposure – particularly exposure for unanticipated transactions. The advent of frontier AI has also opened up a whole new world of possibilities for businesses, based on more advanced reasoning capabilities. Businesses also should pay close attention to AI's move from the cloud to local devices, which raises a series of confidentiality and security issues for companies that have not set out appropriate policies and procedures.

Q: WHAT DOES EVERY BUSINESS LEADER NEED TO UNDERSTAND ABOUT AI RIGHT NOW THAT THEY MAY STILL BE UNDERESTIMATING?

A: TELANOFF:

AI will redefine the way that business is done on a scale that is similar to the changes we saw with the availability of the personal computers and high-speed internet. But these changes do not impact the core responsibility and accountability of business leaders. The buck stops with a human and as good as AI will be, it will still make mistakes, and accountability does not go away.

Q: ARE COMPANIES INVESTING ENOUGH IN THE UNDERLYING INFRASTRUCTURE – DATA QUALITY, CYBERSECURITY, COMPUTING CAPACITY AND SYSTEMS INTEGRATION – TO SUPPORT THEIR AI AMBITIONS?

A: DELAWALLA:

Most small and mid-sized businesses are layering AI tools on top of environments with inconsistent identity controls, unclassified data and limited visibility into who can access what. AI amplifies whatever it sits on: if permissions are messy, an AI assistant will surface sensitive files to the wrong people in seconds. Before scaling AI, companies should clean up access rights, label sensitive data, enforce multifactor authentication everywhere and monitor for account takeover. That foundation is unglamorous, but it decides whether AI becomes an advantage or a liability.

Q: WHAT SEPARATES COMPANIES THAT ARE SUCCESSFULLY DEPLOYING AI FROM THOSE THAT ARE EXPERIMENTING WITH IT BUT NOT SEEING MEANINGFUL RETURNS?

A: TELANOFF:

Companies that understand their business can best determine how to improve their operations using AI in a role that complements their staff. Like any tool, AI can be misused, used for unsuitable tasks and not used when it should be used. The most effective companies use AI as a smart assistant, a great asset for catching the last critical 10%, but never expected to work unsupervised. In our law firm, we can leverage AI to allow attorneys to get the same amount of work in a shorter time, saving clients money. However, while AI can make an attorney more efficient, it lacks the responsibility and decision-making ability that requires human direction.

> *"What is critical is that lawyers, technology people, marketing and the C-suite are all aligned on how a business manages AI governance."*
>
> – IAN C. BALLON

Q: HOW QUICKLY ARE AI AGENTS LIKELY TO MOVE FROM ANSWERING QUESTIONS AND GENERATING CONTENT TO ACTUALLY PERFORMING BUSINESS TASKS AND MAKING DECISIONS?

A: BALLON:

AI agents already perform tasks and make decisions within pre-set parameters or subject to human consent. The move from chatbots to agentic AI has already taken place for larger or more sophisticated companies.

Q: WHAT SHOULD EXECUTIVES KNOW ABOUT THE RISKS OF GIVING AI SYSTEMS GREATER AUTONOMY INSIDE THEIR ORGANIZATIONS?

A: DELAWALLA:

An autonomous agent is effectively a new employee with system access, limited judgment and the ability to act at machine speed. The risks are concrete: agents can be manipulated through hidden instructions in emails or documents, can inherit excessive permissions, and can make errors that spread before anyone notices. Executives should insist on three controls: least-privilege access scoped to each task, human approval for anything irreversible such as payments or data deletion, and full logging of every action the agent takes. If you cannot audit what an agent did, it should not be doing it.

Q: HOW SHOULD COMPANIES THINK ABOUT PROTECTING PROPRIETARY DATA AND INTELLECTUAL PROPERTY WHEN EMPLOYEES ARE USING INCREASINGLY POWERFUL AI TOOLS?

A: BALLON:

IP law remains important to companies – especially those with innovative technologies or business models. AI's use potentially could complicate a business' efforts to assert IP rights in its creations or inventions because music, motion pictures, software or other content created purely by AI are not entitled to copyright protection and inventions (including software apps) created using AI generally are not patentable. Savvy rights owners and their IP counsel understand how to frame potential inventions, creative works and apps to include human involvement. The Copyright Office, for example, will allow works to be registered and given presumptive protection by U.S. copyright law where there is sufficient human involvement in the work's creation. To protect trade secrets and confidential information, companies should not expose their secrets in commercially available AI products. Businesses may wish to license proprietary versions of popular AI applications, but in doing so they or their lawyers need to carefully review license terms to make sure that information accessed is not used to train tools for competitors and that proprietary or confidential business information is not otherwise shared with third parties. Disclosure of a trade secret – even through inadvertence – can destroy its status as intellectual property, meaning others could then freely use or copy it.

A: DELAWALLA:

Start by assuming employees are already using AI tools you have not approved, because they almost certainly are. Banning AI rarely works; it pushes usage into personal accounts where you have zero visibility. You cannot protect data you cannot see leaving. That is why we built Chado, our shadow AI monitoring platform. It discovers which AI tools employees actually use, flags sensitive data such as client records, credentials, or source code entered into prompts, and maps that activity to the NIST AI Risk Management Framework. Visibility comes first. Policy without it is guesswork.

Q: WHAT DOES THE RISE OF AI MEAN FOR THE WORKFORCE? WHICH JOBS ARE MOST LIKELY TO CHANGE SIGNIFICANTLY, AND WHAT SKILLS WILL BECOME MORE VALUABLE?

A: TELANOFF:

The impact that is already being felt is that entry-level jobs have changed. Repetitive tasks that were traditionally used to introduce new employees to a field can be performed faster and with higher quality output by AI. Simply being able to handle paperwork or perform data entry is not enough. All jobs are going to require critical thinking, practical ethics, interpersonal skills and solid judgment. Cranking out drafts or "busy work" are in the past, the ability to direct and evaluate AI production will be the most valuable skill moving forward.

Q: WHO ULTIMATELY OWNS AI RISK INSIDE A COMPANY – THE CEO, CIO, CTO, LEGAL DEPARTMENT, CYBERSECURITY TEAM, OR SOME COMBINATION?

A: DELAWALLA:

Accountability sits with the CEO, because AI risk is business risk. Execution is shared. IT and security own access, monitoring, and incident response. Legal owns contracts, privacy, and regulatory exposure. Business leaders own the decision to deploy AI in their workflows and the outcomes it produces. What fails is the default model where everyone assumes someone else is watching. We recommend a small cross-functional governance group with a named executive sponsor, a written acceptable-use policy and an inventory of every AI tool in use, approved or not.

A: BALLON:

Different companies treat AI governance issues differently. There is no "one size fits all" approach. Some companies create a CAIO, while others assign AI governance to the CPO or the law department or a committee comprised of different stakeholders. What is critical is that lawyers, technology people, marketing and the C-suite are all aligned on how a business manages AI governance. Good AI governance is important to limit liability and loss exposure and to reduce litigation and regulatory enforcement actions.

Q: SHOULD BUSINESSES BE THINKING PRIMARILY ABOUT REPLACING TASKS WITH AI OR AUGMENTING THEIR EMPLOYEES – AND HOW DOES THAT DISTINCTION AFFECT THE WAY THEY INVEST?

A: TELANOFF:

This is not an either/or choice, both are essential. There are repetitive tasks that are best handled by AI, but the core work of any business still needs human intuition and responsibility. In our law practice, we can use AI to review and find patterns in thousands of documents quickly; however, it still requires an experienced lawyer to tell the AI what to look for, to confirm that what AI finds actually matters, and craft a persuasive story to tell a judge or jury. The key is to leverage AI to augment employee performance, not to replace them.

> *Before scaling AI, companies should clean up access rights, label sensitive data, enforce multifactor authentication everywhere and monitor for account takeover."*
>
> – PERVEZ DELAWALLA

Q: WHAT AI-RELATED REGULATORY OR LEGAL DEVELOPMENTS SHOULD BUSINESS LEADERS BE PAYING THE CLOSEST ATTENTION TO AS WE MOVE TOWARD 2027?

A: BALLON:

The evolving legal framework governing agentic AI. Courts are just starting to be called upon to determine whether a user who deploys an agent or the company that created an agentic tool (or both) should be held liable for the acts or omissions of the agent. This question may be answered by ancient common law agency principles, contract law or under state or federal statutes, among other things. The same facts may lead to different outcomes depending on the particular law applied and the given jurisdiction. This becomes complex both for businesses that make agentic tools commercially available and companies that deploy the agents. Businesses that deploy agentic AI tools should consider ways to obtain privity of contract with users to disclose risks, obtain consent to privacy policies, and disclaim or limit liability. By contrast, companies that employ third-party agentic tools need to understand the terms under which a tool has been made available and what processes, procedures and policies to put in place to limit exposure and avoid unintended consequences.

Q: HOW SHOULD COMPANIES APPROACH AI TRAINING? IS BASIC AI LITERACY ENOUGH, OR WILL EMPLOYEES NEED SUBSTANTIALLY DEEPER TECHNICAL AND ANALYTICAL SKILLS?

A: TELANOFF:

All businesses will need both widespread AI literacy and skilled employees with deeper technical and analytical skills. Just as in every office today, all employees need to understand how to use a computer and to have basic computer user skills. Also, just as today, specialists will be needed, just like businesses now have internal or external IT departments. AI will need a new type of specialist, who helps the larger workforce use AI. Managers need to be able to manage both human and AI subordinates, recognizing their strengths and weaknesses.

Q: IF YOU WERE ADVISING A CEO TODAY, WHAT ARE THE THREE THINGS YOU WOULD TELL THEM TO DO BEFORE THE END OF 2026 TO MAKE SURE THEIR COMPANY IS PREPARED FOR THE AI-DRIVEN BUSINESS ENVIRONMENT AHEAD?

A: DELAWALLA:

First, inventory every AI tool and AI-enabled feature already running in your business, including the ones employees adopted on their own. Second, fix your identity and data foundations: enforce multifactor authentication, remove excessive access rights and classify sensitive information, because AI will expose every weakness there. Our AI Exposure Management platform shows exactly what your AI assistants can reach through existing permissions and scores that exposure against the NIST AI Risk Management Framework. Third, pick two or three high-value workflows, deploy AI with clear success metrics and measure results within 90 days.

Q: WHAT IS THE BIGGEST AI MISTAKE YOU SEE BUSINESS LEADERS MAKING RIGHT NOW?

A: DELAWALLA:

Treating AI adoption as a software purchase rather than an expansion of their attack surface. Leaders approve an AI tool, connect it to email, file storage, and customer systems and never revisit the permissions. Meanwhile, attackers are using the same technology to write convincing phishing emails, clone executive voices and automate attacks against smaller businesses at scale. The mistake is not adopting AI. It is adopting AI without asking what it can access, who monitors it and what happens when it is misused.

A: BALLON:

Too many companies believe that AI can immediately replace humans and are downsizing without understanding how AI can achieve efficiencies for their businesses and where human judgment and experience are required. I also see companies using AI in place of human lawyers in instances where judgment, perspective and practical experience are required. For example, I have had clients propose legal strategies for IP cases based on AI recommendations without accounting for the fact that generative AI generally returns the most common answer to a given question, rather than one specifically tailored to a company's unique situation. Don't get me wrong – I am a huge fan of AI and have worked with companies in developing machine learning and AI tools for more than 10 years. I also use proprietary (non-public) AI tools to organize and retrieve documents and information and more quickly identify primary source materials to review, among other things. AI is an incredibly powerful tool for efficiency and innovation. But it is important to know how to use AI tools properly – what prompts to ask, what rules to establish for agentic AI, etc. – and to know when human judgment is required.

A: TELANOFF:

Not understanding that AI is a sea change. Every business is going to be restructured to incorporate AI into every aspect of their business. This is the next step in the evolution of business. The change is on the scale of the creation of the printing press, the typewriter, the introduction of computers, and the ubiquity of high speed internet access – and now – AI is doing the same thing. The biggest mistake is letting employees casually test different AI tools across departments without clear guidelines. Without simple ground rules on what can be shared and how answers must be verified, companies walk right into avoidable risks. Leaders need to set the rules of the road early.

Q: WHAT DEVELOPMENTS IN AI OVER THE NEXT YEAR COULD FUNDAMENTALLY CHANGE THE WAY BUSINESSES OPERATE BY 2027 – AND WHICH EMERGING TRENDS SHOULD EXECUTIVES BE WATCHING CLOSELY?

A: BALLON:

The expanded use of agentic tools by companies will separate those on the cutting edge from those left behind. Businesses need to understand when and how to deploy agentic AI, what permissions to provide, and how much autonomy agents should have. For businesses making available agentic tools to consumers, it is important to have in place agreements with users to limit liability. Conversely, companies employing agentic tools need to understand the risks and potential exposure associated with the tools they employ and how best to frame permissions. While the law governing agentic AI is still evolving, businesses often can protect themselves through contracts and internal policies, procedures and training.

> *The biggest mistake is letting employees casually test different AI tools across departments without clear guidelines. Without simple ground rules on what can be shared and how answers must be verified, companies walk right into avoidable risks."*
>
> – ADAM TELANOFF

Q: WILL AI ULTIMATELY FAVOR LARGE COMPANIES WITH ENORMOUS DATA AND TECHNOLOGY BUDGETS, OR WILL IT MAKE SMALLER COMPANIES MORE COMPETITIVE?

A: TELANOFF:

Yes. Smaller companies will be more competitive because AI is a tremendous equalizer and force multiplier. No longer are large staffs necessary to handle large datasets. A lean, sharp team can now analyze massive amounts of evidence and match the output of an army of corporate staff, allowing small and even single-person operations to take on industry giants head-to-head. Big companies will always have deeper pockets for raw computing power, but smaller businesses are faster, more agile and quicker to adapt. In the end, success won't come down to who has the biggest budget, but who uses the technology with the best judgment and precision.

A: DELAWALLA:

AI is one of the strongest equalizers smaller companies have seen in decades. A 50-person business can now produce analysis, customer service, and documentation that once required entire departments. The catch is that attackers gained the same leverage, and smaller firms rarely have a dedicated security team. Large enterprises will keep their data advantage, but agility favors smaller companies, which can adopt new tools in weeks rather than years. The winners will be those that pair fast AI adoption with security they can realistically afford and sustain.

This supplement was produced by LA Times Studios and is independent of the L.A. Times Newsroom. Contact us with comments or questions at *studios@latimes.com.*