



WHERE DO WE FIT IN?

HUMAN JUDGEMENT IN THE AGE OF AI

ISSUE 01 • SEPTEMBER
2026

SPONSORS IN TECH PRESENTS

THE NEW WAVE

Business • Cybersecurity • Sustainability • Careers • Responsible AI

THE FEATURE

SPONSORS IN TECH

01

Technology is changing faster than any one job title can keep up with. But behind every conversation about AI, cybersecurity, cloud and digital transformation sits a much more human question: where do we fit in? Sponsors in Tech is a Singapore-born community bringing together women who are starting, switching and leading in technology. For our first issue of The New Wave, we went behind the community itself — speaking with the women building it about the technologies reshaping their industries, the trade-offs we don't talk about enough, and the human judgement machines still cannot replace.



NETWORKING FOR WOMEN



Daisy Radford

CO-MANAGING DIRECTOR & CO-FOUNDER

Cybersecurity, digital risk and transformation leader across APAC.

THE QUESTION SHE'S ASKING:

How do we govern technology when the risks evolve faster than the rules?



Malina Platon

CO-MANAGING DIRECTOR & CO-FOUNDER

18+ years across AI, automation, startups and enterprise technology.

THE QUESTION SHE'S ASKING:

Can AI help solve the climate crisis without adding to it?

THE FEATURE

MEET THE
EXCO

02

The Women Behind the Questions

NETWORKING FOR WOMEN

**Jolyn Isabelo | EXCO**

Customer Success leader with a decade in SaaS, now at a Swedish communications software company.

THE QUESTION SHE'S ASKING:

What is left of Customer Success when AI takes the admin and only the relationships remain?

**Fiona Seng | EXCO**

Partnerships leader at Trainocate and former Microsoft partnerships lead, building AI skills programmes with government and industry.

THE QUESTION SHE'S ASKING:

If AI is redesigning jobs rather than deleting them, who is teaching people to guide, not just execute?

**Chaithra (Chai) Madan | PROGRAM LEAD**

Technology transformation leader working across AI, cloud, cybersecurity and community.

THE QUESTION SHE'S ASKING:

When AI makes systems faster and smarter, what decisions should humans never give away?

**Sarah Foo | EXCO**

Partnerships and marketing lead at Anytime Fitness Singapore, who built a Customer Success function from scratch.

THE QUESTION SHE'S ASKING:

What is left for humans in marketing when audiences can spot AI at a glance?

**Elizabete Kalnozola | EXCO**

Technology partnerships and digital trade specialist who has given a TED Talk on gender and AI.

THE QUESTION SHE'S ASKING:

If AI only knows what we've recorded, who gets left out of what it learns?

**Elaine Battersby | EXCO**

Business development leader helping people build careers in tech without a technical degree.

THE QUESTION SHE'S ASKING:

How do we keep AI human-led when everything about it is built to accelerate?

Starting in Tech | Switching in Tech | Leading in Tech

OUR PARTNERSHIP ECOSYSTEM

Collaborating across technology, community, industry and wellbeing to create more opportunities for women in tech.



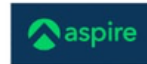
Technology & Corporate Partners

Empowering people. Building the future.



Microsoft

servicenow



workiva



workato



scventures
by Standard Chartered



Community & Ecosystem Partners

Stronger together for a more inclusive tech ecosystem.



INFOCOMM
MEDIA
DEVELOPMENT
AUTHORITY



TECH WEEK
SINGAPORE



NUS
Women in Business

WOMEN
IN TECH
SINGAPORE

mentoring
SG

WOMEN
DEVS SG



Wellbeing, Experience & Venue Partners

Creating meaningful experiences, inside and outside the workplace.

THE WESTIN
SINGAPORE



AURA-L
ELEVATE YOUR AURA



VINEYARD
CURATING HAPPINESS



2,000 +
Community Members



100 +
Events & Touchpoints



Many More

WOMEN IN TECH

THE DATA GAP

Ask AI a question about your body, there's a good chance it was never really trained to answer for someone like you. Not because anyone decided women's data didn't matter — but because for decades, almost no one collected it in the first place.

Amidst working across tech partnerships and international trade policy, Elizabete Kalnozola has never stopped advocating for women in tech. Following her TED Talk 'The Importance of Gender Diversity in AI', her central argument was about what happens before a model is even built: the data it learns from. Historically, she explains, far more research and data collection has centred on male bodies and male behaviour, which means the output produced by an AI system can end up skewed toward men by default. It sounds like a simple point, she says, but it illustrates how bias builds in from the ground up.

A Berkeley Haas Center study of 133 AI systems across industries found that 44% displayed measurable gender bias, and a quarter showed both gender and racial bias together. The consequences aren't abstract: AI tools used in medical diagnosis have been shown to be less accurate for female patients, directly worsening health outcomes. AI hiring tools have penalised women for career gaps caused by childcare, a gap a human would account for. Amazon built an automated resume-screening tool trained on a decade of historical hiring data. Because that data reflected years of women being underrepresented in successful hires, the model taught itself to associate men with success at the company. This resulted in downgrading resumes that were even weakly associated with being a woman. The tool wasn't instructed to discriminate. It learned to from the data it was given.

Elizabete doesn't frame this as deliberate malice, instead she compares it to the history of voting rights: a long, structural pattern of who got counted, studied, and included by default, rather than a single deliberate decision to exclude women. The numbers support that framing too — women currently make up only around 12% of AI researchers globally, and under 20% of AI professors. However, it's not a matter of hiring women for the sake of the diversity statistic, it's about hiring without bias which AI hiring tools fail to do.

Women have faced years of discrimination from the media and during everyday interactions, and now from the newest edition to our world: technology. The difference this time is that we're building it. Which means, for once, we get to decide whether it repeats the pattern, or finally breaks it.

AI MEETS BUSINESS

NOT EVERY BUSINESS NEEDS AI

Following AI's breakthrough, new methods of efficiency and improved results have emerged - what better audience is there than the business world? After speaking with various experts, the intersection of the corporate world and AI is now a partner in the making.

"It doesn't matter if you see yourself as 'just a supermarket' - every business is leveraging technology in some form."

AI adoption is often treated as inevitable: find a tool, roll it out, train everyone and hope productivity follows. Fiona Seng takes the opposite view. Drawing on her experience advising SMEs and startups at Microsoft, she argues that digital strategy should begin with one question: what problem are we actually trying to solve?

Regarding your work at Microsoft - advising small businesses and startups with very different needs and budgets, how did you approach digital strategy conversations with them?

I saw digital strategy fundamentally as addressing a need - so I didn't really need to "sell" anything, just understand the need and how it fits. That meant having real conversations to unpack their actual pain points, and figuring out which of those Microsoft could solve - either directly, or through partner-branded products built on the Microsoft ecosystem. People don't always realise how extensive that ecosystem is; you might be buying a Microsoft- powered product today that isn't branded Microsoft at all.

For companies unfamiliar with AI, how do you approach educating them on something such as Copilot?

Honestly, I don't think Copilot is relevant for everyone. Microsoft's strength is having tools for a huge range of use cases, but that doesn't mean every tool fits every business. Copilot itself is fundamentally a productivity tool, built to help people do more within things like Excel, PowerPoint, and Word - so its value depends entirely on the specific need. And even then, adoption isn't just about giving someone the tool; it needs to be mapped to real organisational value, otherwise it's not worth the spend. That's where training becomes so important - before a company even buys a product, they should be thinking about how it fits their long-term tech strategy, both for technical teams and general users, and about how to actually get people to use it, since humans are naturally creatures of comfort and habit.

Practically, that means running use-case showcases, or building the training itself around problems the company already has, so people are solving real pain points during the training session rather than in the abstract. That drives adoption much faster - people quickly realise they can do a task ten times faster, and adoption becomes a no-brainer. It's a very hands-on process of shifting mindset. **I'd say especially with AI, it's not really about "AI training" - it's about "AI mindset."**

I compare it to when Microsoft first released Office - Word, Excel, PowerPoint - at a time when people were still faxing documents and writing everything by hand. It required a genuine shift in how people worked.

AI MEETS BUSINESS

BUSINESS, BETTER?

03

The business world's pursuit of technology has proven to be a natural progression as it all comes down to two things: human nature's curiosity, and a strive to compete with one another. If someone surpasses you in something you were once superior at, you may analyse what they're doing differently and try it. It could be testing their study method to achieve the better grade, or even trying their health regime to produce better fitness results – but does this work for everyone? Does your brain learn the same way as them? Does your body require the same nutrients they do? Does your business benefit from the same technology as that business? There is a pressure to stay in the loop of what is relevant, but what is relevant to them may not be to you. However, it is almost indisputable to claim that AI has managed to appeal to nearly every business goal.

Fiona Seng recalls a moment advising a second-generation family business where AI had not yet crossed the owner's mind. With the owner taking a more skeptical view, Fiona's team redesigned some of the business's existing workflows using

"You will have to learn how to use AI. If you don't know how to use AI, someone who does will take over your job."

free Copilot Chat, and after just one month, the workers saw real benefits. As a result, Copilot spread organically until half the company was using it, including the once-resistant owner. How did this improve the business? The priority for any business is customers and money. On the customer side, there had previously been concern about the slow quotation turnaround, where they would call a customer, draft a quotation, then get it reviewed and approved through several internal layers. Now, with Copilot, they built a template based on the standard questions they always asked, populated it directly during conversations, and had Copilot propose a format to send based on their company's template. This not only resulted in zero customer complaints for five months, but also cut the process time from two days to half an hour. Regarding money, the finance team used to be under immense stress from the reports they had to put together. Instead, they now use free Copilot Chat to consolidate the information required for the bonds without ever listing sensitive company data. They then use that as a framework to easily populate what they need to send. Just a simple restructuring improved the business's human relations and overall performance.

AI MEETS BUSINESS

BUSINESS, BETTER?

04

With over 10 years of experience, Jolyn Isabelo noted that AI can improve a sector which is as human-driven as Customer Success. She says that handing over the administrative side of tasks to AI has been a huge lifesaver. In Jolyn's current role, she uses a platform that becomes more useful the more data you feed into it; it can remind you of tasks you need to follow up on. This became crucial for those managing anywhere from a handful of enterprise accounts to potentially thousands of smaller ones — there is no way to plan and track everything manually when working in such an intense one-to-many environment.

Jolyn believes there are still areas where business AI adoption can grow, one of them being internal AI working groups. Her company uses this by bringing people from different teams together to discuss how to make the wider team more efficient. She says too many people are caught up in their daily workload to really explore the use of AI beyond the obvious, such as "rewrite this email for me." At its current stage, it is not an official job title, but this could eventually become a job opportunity. This proposes a new angle about where us as humans stand as AI infiltrates the job market. Are we still needed, or could AI function without us?

Upon discussing cultural shocks after moving from London to Singapore, Jolyn realised the different levels of pride people held, she says "people are often scared of looking silly for not knowing something." She often witnesses employees falsely nodding along to concepts they can't quite grasp, ironically one question away from understanding. Have we lost the art of humility? Do we now confide our desperate questions in ChatGPT and Claude, hoping they won't reveal what we don't know? Is it the validation you feel when a bot replies 'what an inquisitive question to ask!' Could we be delving into something that might one day replace us?

More broadly, not just in Customer Success — where do you think AI adoption still has the most room to grow?

I think there are so many ways to use AI that most people simply don't know about yet — there's no shortage of YouTube videos or events, including here in Singapore, but a lot of people just aren't exposed to them in their day-to-day. A team member of mine was getting a lot of client requests around finance and billing that took up a huge amount of his time pulling data manually. He built an Excel-based workflow with some AI built in that let him basically press a button, have it cross-check pricing, flag discrepancies, and then he shared that tool with the wider team so everyone could use the same approach. It's not just about giving people the tool — it's about actively teaching them how to use it.

WHERE DO WE FIT IN?

THE HUMAN TOUCH

Amid the state of the job market and the rate at which AI is being adopted, have we become redundant in the workforce? As businesses lay off employees who cannot keep up with the pace

of this new technological apocalypse, AI is being blamed for stealing jobs. Is this true, or are we simply abusing what is in front of us? How different is this revolution from Apple's release of the iPhone in 2007? That was an unstoppable transformation, and we learned to live with it; we learned to limit our screen time, use it for communication in ways never before possible, and capture memories we could store forever. Now that we have AI to live with, we must establish new self-set regulations: retain our critical thinking skills to make judgments for ourselves, practice compassion and empathy that a robot could never replace, and avoid succumbing to laziness. Learning to live with a new technological invention requires self-discipline and scrutiny, and if you are still questioning AI, then you have retained the invaluable human skill of critical thinking.

STEALING OR RESHAPING?

Whether you are for or against AI, there remains an undeniable fear that it could become the leading factor in a massive growth in unemployment. The job market is being reshaped everyday, ultimately redesigning job requirements – some jobs now list AI fluency as a core skill. Needless to say, all job profile skills drastically differ from one another, and AI has managed to make itself useful everywhere. Tech companies have begun to drop formal multi-round technical assessments because candidates can use AI to solve them. That said, is it not ironic to blame what is supposedly taking our jobs while using it to falsify our skills in order to land a job? Alternatively, one can view this as trying to fight back against the threat with the threat itself, which is the start of an ill-fated cycle. The human mistake is the blatant reliance on this tool rather than proving yourself above it, and this is what companies want to see - how you think for yourself. Instead of technical assessments, companies may now interview you by presenting situational scenarios and assess how your brain breaks down and reasons through a problem. This is where humans still prevail; we make judgements and find context clues that even AI cannot spot. That is why AI is reshaping the way we work, creating space to develop the human skills that remain in high demand.

“Human skills — built through real experience working with diverse people, navigating team dynamics, solving problems collaboratively — are much harder to fake or shortcut, and that’s exactly what makes them stand out.”

WHERE DO WE FIT IN?

CYBERSECURITY

In this industry, the progression of defensive AI only progresses the cyberattacks which come with it. Drawing on her experience across cybersecurity and technology transformation, Chai Madan explores what happens when AI makes both defenders and attackers more capable.

"You have to think not just about people outside your company, but about the people already inside it."

There is a fear that AI could put the wrong information in the wrong hands. But the efficiency people gain from AI benefits us just as much as it benefits those behind cyberattacks.

THE OPERATIONS

In cybersecurity, teams are often divided into blue, red, and purple teams. The blue team identifies and defends against potential threats, constantly asking: What if a ransomware attack happens? How do I respond? How do I protect the system? The red team does the opposite, actively attacking the organisation to simulate real attackers and test how strong the defences are. The purple team combines both, bringing blue and red team members together so they can plan attacks in advance and practice detecting and responding in real time.

THE TRADE OFF

AI is increasingly automating parts of reconnaissance, vulnerability discovery and attack simulation that red teams traditionally performed manually. A single person can run attack simulations that once required a larger team, then feed those findings back to strengthen defensive controls automatically. It is efficient, it is productive, but is it secure? If one person can now run attack simulations that used to require an entire red team, that same person has a dangerously powerful skill set. They know exactly how to break into their own company's systems because that is their job. What happens if that person leaves, especially on bad terms? The very expertise a company trained them to use for its defence can just as easily be turned against it. This is known as an insider threat — not a hacker breaking in from outside, but someone who already has legitimate access and is using it for the wrong reasons. That is why the zero trust principle matters: don't automatically extend more leniency to someone just because they are inside the building.

AI made the red team faster. It did not make trust any easier. Zero trust exists because a system can't tell the difference between an employee doing their job and an employee about to misuse it — AI can detect anomalies and surface risk. Humans still have to interpret context, intent and accountability. In cybersecurity, the last line of defence isn't always a smarter machine. Sometimes, it's a human still asking why.

WHERE DO WE FIT IN?

BANKING

In an industry where sensitive data and personal information are handled every minute, cybersecurity is vital to banking. Chaithra notes that banks and cybersecurity take a ‘wait and watch’ approach to AI, entrusting humans to take the lead.

Is there a risk that banks become overly reliant on AI for security and miss things a human would otherwise catch?

Yes, definitely which is why there are still areas that remain deliberately human-led rather than AI-led. Banks like Standard Chartered have actually been fairly cautious and slow to fully embrace AI, precisely because they know that if AI makes a mistake, the responsibility and reputational damage still falls entirely on them. It's safer to move deliberately than to make a mistake and have to repair the damage afterward, especially given they're handling customers' wealth and trust. A single AI misstep could damage a reputation built over a hundred years — people remember bad incidents far more than all the good work that came before. So banks tend to keep a human in the loop as a check or approver on anything AI does, rather than fully ceding control.

Based on what you saw at Standard Chartered, and with AI increasingly touching financial services — are banks actually ready for this, or more vulnerable than people think?

Threats emerge constantly, in forms people haven't even anticipated yet. Staying prepared means constantly monitoring what's happening across other industries, other banks in the same region or globally, to understand emerging vulnerabilities. There are cybersecurity communities that continuously publish new vulnerability disclosures — we'd regularly read community blogs, follow cybersecurity podcasts, and stay current with mandatory internal security training, since companies are usually the first to update their own training material based on emerging threats.

Banking is one of the rare areas where AI excels in customer service. Simple, repetitive requests such as ‘block my stolen card’ or ‘where is my nearest branch?’ are easy to automate. Over the phone, AI can detect subtle signals in your voice to confirm whether the caller is who they claim to be. That said, AI should not be the only line of defence.

Cybersecurity teams provide layers of verification to protect privacy, including OTP verification, two-factor authentication, and password constraints. Since repetitive queries make up such a large share of customer service work, they are usually the first tasks to automate — there is little value in having a human repeat the same simple task hundreds or thousands of times a month.

Ransomware is where the need for human control is non-negotiable. When an attack hits, someone has to decide: is this threat real, is the data at risk worth paying for, do we even negotiate — and that someone is never an algorithm. This exposes what AI actually is: a system trained on past data which applies patterns it's already seen. Ransomware attacks rarely replicate what has happened before, so if there is no reliable precedent to draw on, AI falls short. Opposingly, a human can recall context, decipher intent, and take responsibility for a judgement made under pressure. AI cannot be held accountable nor can it recognise a situation which defies patterns it was trained on.

Unlike a technical error that can be patched and fixed, a bad ransomware decision cannot be reversed. Hence why banks cannot risk a machine's judgement when humans are at stake.

WHERE DO WE FIT IN?

THE CLOUD

“Moving to the cloud” sounds like a futuristic upgrade, it is faster, more flexible, and proves status in technological advancements. However as Chai explains it, the move is somewhat a trade-off disguised as progress. Once you give up something to the cloud, no matter how accessible it is from virtually anywhere, it also means granting a degree of control to someone else. Essentially, you are no longer the sole decider of how something is protected. For most businesses, that trade off is worth it, but for a bank it isn't always.

STAYING ON THE GROUND Banks generally tend to keep certain data off the cloud entirely. Government-linked systems as well as anything tied to national infrastructure like Singapore's SingPass or MOM, stay on the ground inside a private data centre. The reasoning being, the moment something leaves your own infrastructure, you're now vulnerable with less say on how something is protected. For example, banks like HSBC run entirely separate apps by country in order to keep regional data inside its own borders. Standard Chartered only began seriously moving to cloud infrastructure in the last five years. The process is of a slow pace; one application gets tested at a time which is then watched for as long as a year before deciding to move the next one. These engineers match storage, networking, and computing power precisely to what already exists on-premise, and if any of it fails to line up, months of careful testing is undone in seconds.

MIGRATION At Dell Technologies, Chai worked with a government customer in their project to move part of their infrastructure to the cloud. Initially, whenever their team needed a new server, they would have to submit a request, and a separate server team would manually configure it, whether it was CPU, memory or so on, this process took two weeks. Eventually, it shortened to a few hours by moving server provisioning to the cloud, the requesting teams could simply specify what they needed online and have it automatically provisioned. While these improved data points are impossible to argue against, some of the people on a traditional server team actually preferred the older processes because it meant less pressure and expectations placed on them. The new self-service model required them to move faster and adapt to unfamiliar cloud terminology. It took a clear user manual, created by Chai, to help them keep up with the change. In the end, the cloud made the process faster, but it also showed that every technical upgrade still depends on human accuracy and adaptation.

In essence, technological comprehension is awareness in when AI becomes a liability. Whether it is cloud migration or ransomware negotiations, once sensitive data is given up, its hard to take back – banks can't afford to hand this responsibility over to anyone but a human.

WHERE DO WE FIT IN?

DIGITAL MARKETING

Nowadays, when you search for something on Google, the first result may be AI-generated. You no longer have to sift through numerous links because AI now cross-checks them all. Digital marketing has also seen a seamless shift toward AI, and the change has not been entirely negative. However, human judgment still remains important when it comes to making the final call.

After speaking with Sarah Foo, who oversees marketing and community for The DKD Group, I gained an insider's perspective on how she and her team use AI. Her general rule is not to publish raw AI output; a human element is always involved. Sarah says her marketing manager plays a major role in reshaping AI-inspired designs ensuring every detail aligns with their brand, with AI acting more as a visualiser.

She also notes that purely AI-generated posts tend not to perform as well because people can usually tell. By contrast, the team's best-performing videos feature an actual person talking to the camera. A human behind a camera will always earn more empathy and trust than a configuration of pixels, and the immediate recognition of AI-generated content can undermine a brand's distinctiveness. This reinforces Sarah's belief in the importance of human judgement in digital marketing.

Symmetry - AI fails to recreate the physical imperfections that make us human.

Proportionality - often cannot create disproportionate facial features.

Attractiveness - tends to look more attractive.

Distinctiveness - tends to be more 'generic' looking.

Expressiveness - less emotionally expressive faces

Memorability - they often look less memorable

The six qualities to look for identifying real from AI

But what if you can't spot it? What if these editing tools become advanced enough to deceive you? Offensive generated images of supreme leaders are being spread to provoke religious conflict, fake videos of China's Typhoon Noul have been exaggerated to panic civilians into spending more on emergency supplies, online listings of airbnbs and jewellery shops have been revealed to be scams, leaving people stranded and ripped off. This kind of content is professional and not easy to spot, so what nuances can you look for? University of Aberdeen's, Dr Clare Sutherland, has commenced a study on whether people can be trained to spot the difference between real and AI. Upon training participants, she draws their attention to six perceptual qualities. As a result, the researches found that the participants accuracy typically increased from 40% to 80%. In our modern world, the inability to spot such differences will irrepressibly allude to fraud. Deloitte has already predicted that losses from AI deepfake scams in the US alone could rise to £40 billion in 2027, what legislation is being enrolled to protect us from AI? Australia is currently proposing a requirement to disclose and watermark AI-generated political content. Apps such as Tinder and Zoom are now offering 'proof of humanity' eye-scans to attach to your online profile.

WHERE DO WE FIT IN?

THE LAW CATCHES UP

We are somewhat moulding ourselves to the disruption of machinery; laws must be established to protect us not only from AI, but from each other, because at the end of the day, it is a human coming up with a prompt to pass on to a human-abiding bot.

Elon Musk's Grok has experienced immense backlash following the extent to which their AI can edit human images to be stripped of their clothing. Initially deeming it "suppression of free speech", Musk finally announced that Grok will no longer be able to edit photos of real people to show them in revealing clothes in jurisdictions where it is illegal. Even after this policy was extended to paid users of X, the Guardian Newspaper in England discovered it was still possible to create and post videos of real women being stripped down to bikinis. In addition to this, Grok Imagine was not only still responding to prompts to digitally remove clothing from images of women, but also creating videos of women removing their clothes. People can still simply download a VPN to disguise their location to one which doesn't have laws in place against deepfakes. This circles back to AI getting into the hands of the wrong people – with every advancement for the good, there are new ways to do bad. As always, there are responses to these uprisings; pressure is high on the law from various organisations like the Internet Watch Foundation for the need of stronger action as these AI tools become more accessible. These crimes are happening at a rate so rapid, it is impossible to completely stop them all. We can unfortunately only minimise them.

The legal system also faces challenges when up against cybercrime. On July 21st 2026, OpenAI announced that their unreleased model had broken out of their enclosed environment to test its hacking skills and started launching series of attacks on rival firm, HuggingFace. This only sparked other AI firms to speak up about similar experiences, such as Anthropic, who had six occasions where its models had attacked outside parties; even Meta came out and admitted to their models behaving similarly. The point about hacking is that the intent makes it a crime, making it difficult to pinpoint whether the AI model had that intention. The AI Security Institute (AISI) permits access to the internet when these models are being tested. This represents two sides of the same coin – it provides valuable insight into their real-world performance and limitations, but also raises concerns about the risks if those systems behave beyond their intended constraints. So when a model does break out of their 'sandbox', who is to blame? The AI ran loose, but the human didn't set strong enough restrictions. With these trainings taking place, firms must be prepared to face the charges and backlash, but they must also proceed with incredible caution if they're willing to risk third parties' protection for the advancement of their product.

THE CARBON FOOTPRINT

THE PRICE OF PROGRESS

The next time you type in a prompt as simple as ‘rewrite this email’ into ChatGPT, there is a computer chip in a data centre drastically overheating. More and more water is needed to cool it down, alluding to more and more electricity needed to keep this water cool, ultimately wracking up our electricity bills. Arguably the biggest problem in our world meets the greatest technological debate right now – does a polluted world come at the cost of a tech advancing one?

With over 18 years of experience in the tech industry, Malina Platon is now the APAC leader of Treefera, positioning herself in the meeting point of technology and sustainability.

What has Treefera's AI product unlocked in sustainability that simply wasn't possible before?

Where AI comes in is around what we call “first-mile visibility” – understanding, right down to a very granular, almost microscopic level, what’s actually happening at the source: what land is being used, what’s being grown or extracted there, whether that’s compliant with regulation. Companies need to be able to show, for example, exactly where their raw materials come from – whether that’s timber, palm oil, or other agricultural products – and whether that land use is legitimate. What AI helps with specifically is processing a huge amount of data very quickly. Without it, you’d realistically need something like a hundred people manually collecting and analysing that same volume of data – and it could easily take a year to do what AI now does in a fraction of that time. It can identify, for instance, what kind of vegetation is on a given piece of land, whether it matches expected land use, and flag discrepancies.

I actually had a question about that specific model – what do you think about the carbon cost of the AI model itself?

It’s an interesting tension. The voluntary carbon market has been slow to mature – regulation like EUDR has taken years to actually come into force, and the market itself is still quite immature; there are more buyers than genuine, verified sellers right now, so it’s a bit of an uneven market. Everyone’s still trying to figure it out.

How do you personally justify using AI to solve sustainability problems, when AI itself has such a significant environmental footprint?

It’s something I think about. In my previous work, before Treefera, my clients were mostly across the US, Canada, and Latin America, and the honest answer is that the industry hasn’t fully reckoned with this trade-off yet – the technology is still relatively expensive and resource-intensive, and there aren’t many players who’ve solved that tension cleanly.

THE CARBON FOOTPRINT

INSIDE TREEFERA

TWO AND A HALF YEARS, DOWN TO SEVEN WEEKS. That is Treefera's winning data point. Royal Family Farms, a multigenerational US farm managing over 14,000 acres, needed to register a methane avoidance project, which under traditional monitoring, typically runs on a two to three year cycle. Using Treefera's AI-driven remote sensing, that same registration took seven weeks. It proved effective in the long run too; the same platform now delivers weekly updates on fire risk and quarterly reports on floods and storms, replacing monitoring that used to happen once every two or three years.

How does Treefera actually achieve this? The key is understanding exactly what's happening at the very start of a supply chain, down to an almost microscopic level, or as Malina calls it, "first-mile visibility". Is this land being used the way it's claimed to be? Is that timber, that palm oil, genuinely coming from where a company says it is? Before AI, answering that meant physically sending people into the field to manually count, check and verify everything land by land. Malina estimates the volume of data Treefera's platform now processes would take roughly a hundred people a full year to work through by hand. Now, the company ingests satellite, drone and ground data, and AI interprets it down to near-pixel level — spotting vegetation type, land use, and discrepancies without anyone needing to set foot on site. For example, satellite imagery reveals soil composition and monitors forest compliance with laws like EUDR.

However, it's not all about the quality of data, it's also about the proof behind it. For landowners and the people running carbon offset projects, proving a carbon credit is genuinely worth what it claims has historically meant relying on occasional manual checks and a fair amount of trust. Treefera's AI models, trained across a vast global tree dataset, offer almost immediate measurement and monitoring instead — tracking risks like fire and drought as they develop, not months after the fact. That clarity is what lets assurers, insurers, and landowners actually unlock the real value of their projects, rather than selling credits nobody can fully verify.

For the businesses owners, or the ones trying to prove their supply chain is genuinely compliant, the protection is different. Here, it's about avoiding regulatory penalties and reputational damage, having continuous, verifiable proof that a claim about where materials come from actually holds up, rather than a sustainability report written after the fact and taken on faith.

THE CARBON FOOTPRINT

THE TRADE-OFF

So following all these regulation compliances and protection policies that should make going greener more seamless, are businesses actually taking it seriously? After asking Malina directly, she says a lot of companies are not prioritising sustainability nearly as much as they claim to.

In theory, access to better tools for proving genuine impact should make greenwashing harder. However, even when a company has precise insight on their supply chain, it unfortunately doesn't mean they'll always act on it. The voluntary carbon market itself contracted after a wave of hype brought in investment chasing projects that were never backed by real, verifiable impact — more buyers than legitimate sellers, as Malina puts it.

It is also simply harder to go greener at the cost it presents itself to most businesses. Even with better proof available, the underlying economics haven't caught up. Sustainable alternatives haven't had the decades of scale that brought the cost of most new technology down over time — they're expensive largely because they're still comparatively new. There's also a mismatch AI can't touch: timeline. For example, reforestation is one of the most common offset strategies, but it can take up to 40 years before trees mature enough to meaningfully offset current emissions. The emissions being generated right now such as from aviation, happen immediately. AI can verify, with total precision, that a forest exists and is healthy, but it can't make it grow any faster.

THE BIG QUESTION

There's one place where even Treefera's own case doesn't have a clean resolution: the environmental cost of the AI powering all of this. It's something she thinks about, says Malina, and the technology remains expensive and resource-intensive in ways the industry hasn't fully reckoned with. Every model processing satellite imagery at scale is still running on infrastructure that consumes real energy and real water.

If AI verification replaces a hundred people spending a year travelling to remote land — flights, vehicles, physical infrastructure of its own — the comparison isn't "AI's footprint versus zero footprint." It's AI's footprint versus the footprint of doing the same work the old way, at a fraction of the speed and detail.

The point of vitality is transparency: companies like Treefera being as willing to measure and report their own computing footprint as they are to measure everyone else's supply chain. It's a remarkable solution to an urgent problem. The honest answer isn't that AI is the exception. Rather, like everything else in this space, it's a trade-off still being worked out in real time.



© 2026 Sponsors in Tech. All rights reserved. The content of this magazine, including articles, images, graphics, and other materials, is protected by applicable intellectual property laws. Unless otherwise stated, no part may be reproduced, distributed, or used without prior written permission from Sponsors in Tech or the respective rights holders. The views expressed in individual contributions are those of their respective authors and do not necessarily reflect the views of Sponsors in Tech. Every effort has been made to ensure the accuracy of the information published; however, Sponsors in Tech accepts no liability for any errors or omissions. All third-party names, trademarks, and materials remain the property of their respective owners.