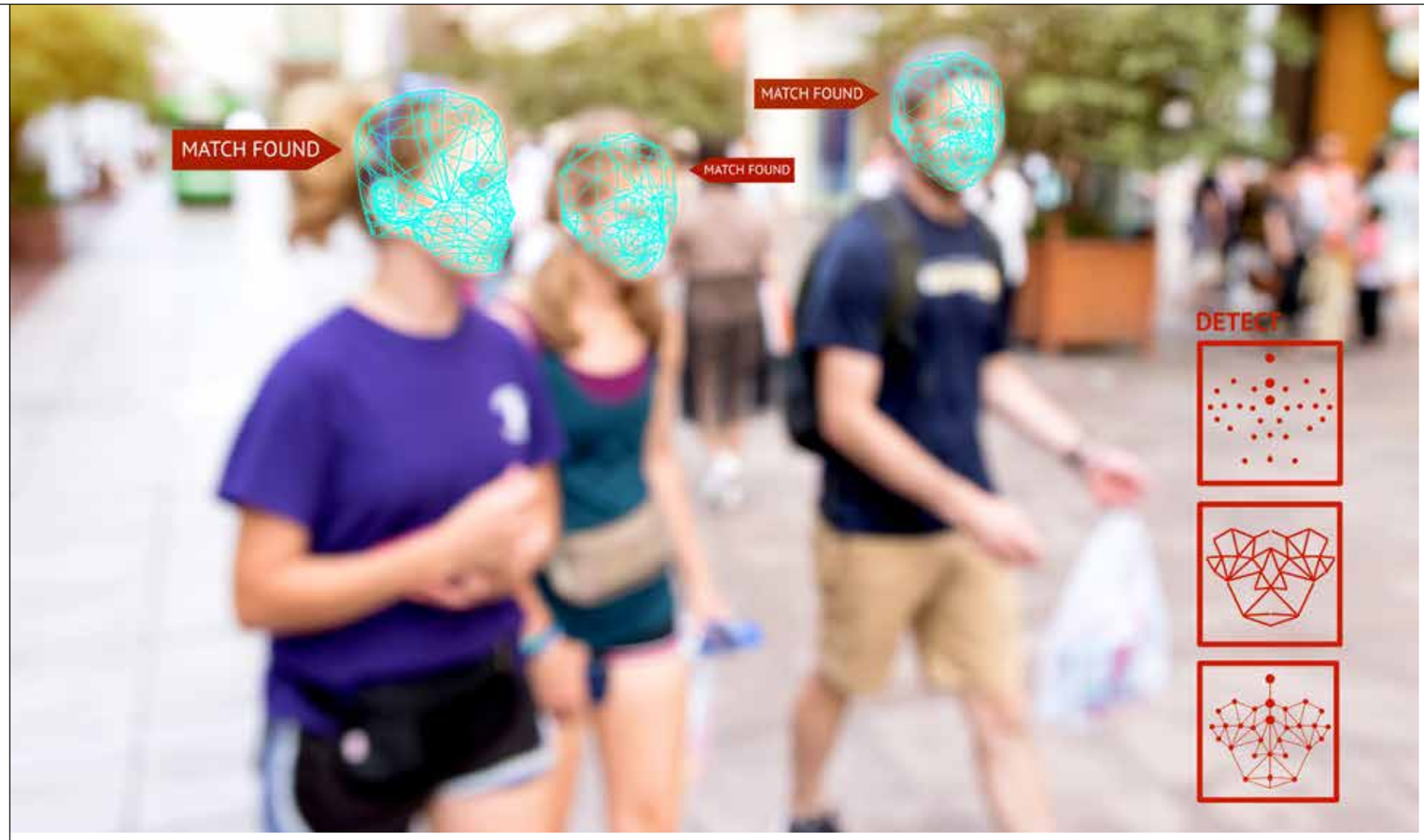

Picture credit: AdobeStock

AI-SPY

REDEFINING SURVEILLANCE – THE RISE OF ETHICAL AI IN VIDEO SECURITY

Mats Thulin *discusses the delicate position of artificial intelligence within security and surveillance – and the importance of getting it right*

Artificial Intelligence is no longer the next big thing. It has, as all new technologies do, made its way through the hype cycle, from initially inflated expectations to inevitable disillusionment – but it has now proven itself ready to deliver. AI is transforming the video surveillance industry at a pace few could have foreseen. The analytics, automation and insights made possible by ever-more powerful hardware and diverse smart software techniques give surveillance an edge it has never had before.

But these advancements come to an industry which has long faced close scrutiny. AI is high stakes: while it offers real operational benefits, it also magnifies privacy and ethics concerns, and cannot be allowed to grow unchecked. Without sufficient care and control, large-scale AI deployment threatens to have a significant societal impact far beyond that of traditional security.

AI deployment has surged over the past two years. Growing demand and deeper application knowledge have cemented AI's utility, but without direction, it is as much a threat as a benefit.

The fast development of AI means it is often not fully understood. Deployment processes and best practices are therefore still evolving – and the industry is well aware. 61 percent of those surveyed between the channel and the end market highlight cyber security, risk and privacy as one of the most significant trends shaping their industry right now. Throwing AI into this already sensitive space is highly unlikely to assuage those fears. The central question, then, is: how can the world deploy and maintain surveillance AI in a responsible and meaningful way?

The future of AI in surveillance will be defined by ethics first and foremost

The core of the answer lies in positioning. The future of AI in surveillance will be defined by ethics first and foremost; in product development, architectural innovation and cross-sector collaboration, ethical considerations must make up the very core of industry practice. Despite what the pace of AI's expansion might suggest, responsible AI doesn't begin after deployment. It begins at the design phase, embedding values such as fairness, transparency and accountability into the technology itself.

In an environment increasingly dominated by prediction, automation and machine intelligence, developers must prioritise humanity. All automated systems need to be backed up by sufficient human oversight. AI has to stay within its boundaries. Developers and stakeholders must be able to explain how AI systems make decisions, and who is accountable should things go wrong. This explainability is critical not just on a technical level, but for maintaining legal and regulatory compliance.

Facial recognition, to offer a prime example, offers significant benefits for active security measures like watch lists, the reduction of activities like shoplifting and the protection of workers. But if AI-powered facial recognition algorithms cannot be aligned with privacy regulations and deployed with full transparency, they risk reputational damage to the technologies and their users. There is no sense in abandoning something so powerful for fear that AI will take things too far – the path forward is to guide its use within ethical frameworks and under the auspices of clear governance.

Equally essential is bias mitigation. AI trained on unbalanced or limited datasets can perpetuate harmful stereotypes, skew risk assessments or produce excessive false positives. Surveillance systems must be rigorously tested to ensure they perform fairly across demographic groups, geographic contexts and edge cases.

Trust, ultimately, is the currency of AI adoption. Privacy, data protection and regulatory compliance are non-negotiable pillars of the security industry. Placing ethical considerations on such a pedestal and allowing them to drive the development of new technologies ensures that even the most technologically advanced AI systems will be able to gain public acceptance in the most technologically conservative markets.

Historically, video surveillance had a clear focus on crime prevention and security monitoring. Even before the rise of AI these boundaries had been somewhat breached and they have now been fully demolished. Surveillance now supports diverse business functions far beyond what legacy systems could have achieved.

The camera itself has been reframed. It's a sensor, a peerless data collector capable of streaming millions of data points every second. Increasing processing power means a camera is a computer, able to interpret that data and generate essential business insights on the fly. And with AI, the camera is a source of curated intelligence, able to transform what it sees into action and efficiently integrate its findings with other data sources.

Consider, for example, a smart city using AI-enabled video analytics to manage congestion. Video feeds integrated with environmental data and real-time alerts offer such a city the ability to reroute traffic dynamically, improving flow and reducing emissions. In retail, AI analysis of video data can map out customer movement patterns to improve store layouts and staffing arrangements. In manufacturing, camera and machine sensor data can work together to highlight production issues, ensure safety compliance and improve operational workflows.

WE ARE ONLY ON THE CUSP OF THE BIGGEST CHANGE THE INDUSTRY HAS EVER SEEN

Today, video surveillance plays a critical role in strategic decision-making which reaches far beyond its traditional scope. But this evolution requires a shift in mindset from a narrow, classical view of surveillance to one that embraces data intelligence as a force for good. And as we broaden the scope of surveillance yet further, it is imperative that all involved with and making use of such technology remain vigilantly within ethical guardrails. More data, more responsibility – it is up to stakeholders to maintain privacy and civil liberties even as use cases expand.

Just as security has moved to a general intelligence role, its architecture has also changed structurally. The client/server model of yesteryear, where individual cameras fed back to centralised servers, has been fast eroded by the processing power of today's camera hardware and the ready availability of online computing provision. The industry is rapidly shifting to a hybrid model, one which takes advantage of the immediacy of edge processing and the scalability of the cloud. This evolution is a key enabler of real-time responsiveness and efficient data management.

AI and machine learning on the network edge enable low-latency-on-device processing supports a faster real-time response. The cloud offers users long-term storage, large-scale distributed analytics, and smooths integration with other enterprise systems. The hybrid model offers the best of both worlds, combining immediacy with historical context, enabling the implementation of granular analytics but also the broad and unified connectivity of remote locations.

At the same time, the hybrid model presents further need for safe, ethical, guardrailed AI applications. A hybrid system lacks definitive central control by its nature. This is not to suggest that such applications are left unchecked, but that anything running on the network edge needs to be developed and tuned with an eye to remaining within all applicable regulatory and moral boundaries. Use of the cloud, transporting sensitive data off-site and operating on hardware often controlled by a third party, necessarily means accepting a certain level of data risk.

Prioritising ethical considerations can mitigate much of this risk. Data need not only be analysed by well-tested, properly controlled AI systems on the network edge, it can also be fully anonymised at the point of collection, before leaving the local network. Designing systems around a hybrid architecture means improved

reliability, scalability and cost efficiency – but it needn't mean compromising on security or privacy.

Where we go next will be defined by unity. These moral imperatives are not a concern reserved only for those developing AI engines or deploying them on security hardware. They are not just a worry for end users putting the future of their businesses in the hands of these applications. Everyone – from technology vendors, system integrators and regulators to end users – has an obligation to contribute to a combined effort to get AI right.

AI TRAINED ON LIMITED OR UNBALANCED DATASETS CAN PERPETUATE HARMFUL STEREOTYPES

Standards for data sharing, interoperability and integration are critical. Without them, innovation risks becoming fragmented and inconsistent. Cyber security has a strong role to play, protecting against interference and poisoning of AI data and, equally, the rise of AI-driven malware, able as it is to morph and adapt to break through static defences.

Through collaboration, the industry can ensure that AI solutions are both technically robust and aligned with regulatory, social and ethical norms. Regulation is catching up – governments globally are establishing boundaries around high-risk AI use. Proactive compliance is an integral component of the long-term viability of AI systems.

Collaboration should cross disciplines. Engineers need input from ethicists. Product designers should be influenced by the concerns of regulators and civil activists. Vendors must communicate with users about the effects of AI, and users with their communities. We need to talk, freely and openly, about both the benefits and pitfalls of AI. This is a major cultural shift, but key to creating AI systems that are truly trusted, transparent and resilient.

At times, it feels as if we have already travelled through a period of major change. And we have, in a sense, following the introduction of ever-smarter hardware and analytics – but the truth is that we are only on the cusp of the biggest change the industry has ever seen. AI and machine learning have the potential to drive not just technological change, but world-altering societal progress. Yet the success of predictive models and smart data analysis hinges on how thoughtfully we, as a society, implement it.

We stand at a crossroads. Take the correct path and users benefit from greater efficiency, improved safety, and the ability to make strong, informed decisions. Get it wrong and every industry, not just security, risks eroding public trust and violating fundamental human rights. The choice belongs to all of us, those manufacturing, designing and implementing security systems. It is up to us to lead the industry into the future and to set an example for the rest of the AI world.

In an industry which is moving forward responsibly, ethics play their part in every step of the design, manufacturing, distribution and deployment process. Hybrid design is embraced, with leaders supporting safe, responsible implementation. Healthy collaboration becomes the norm across the ecosystem, with all parties bound to strong moral guidelines that put people first.

After all, AI's place in the world is not to take over. It is to augment human intelligence, serving the greater good with data insights that allow us to move faster, act smarter and learn more about the way things work. It is not a threat to security, nor an all-encompassing boon. AI in surveillance is a way for us to find and achieve a balance between security and freedom, to build intelligence while maintaining integrity. The question is no longer what AI can do, it's what it should do to earn its place in a smarter, safer world ●

Mats Thulin, Director of AI and Video Analytics, Axis Communications is responsible for development teams working with long term technology and platform development. Mats joined Axis in 2010 and has worked in several roles in technology development.

Video surveillance plays a critical role in strategic decision making far beyond its traditional scope