Thought Networks

EXECUTIVE EXCHANGE

Expert insights on surveillance in the age of AI

The disruptive power of AI in communications surveillance

ROUNDTABLE 1

'AI is already part of daily life, and the adoption curve for AI technologies is accelerating. What feels unwieldy and challenging today will become business as usual tomorrow. We are at a place of change, where the use of AI in driving more targeted surveillance models will not simply bring operational efficiencies and benefits in identifying and managing risks, but will be essential to keep up with the changing world."

SHLOMIT, VP DATA SCIENCE, SHIELD

Thought Networks

Accelerated change: AI and machine learning investment has increasingly been paying dividends, with accelerated capabilities and subsequent operational efficiencies in the last two years. First movers in AI communications surveillance adoption recognise that the technologies are rapidly evolving and will significantly change, but the upward trending of false positives means late adopters risk being left behind, with rule-based surveillance systems at risk of obsolescence. Many firms are exploring or have established a hybrid model, where AI and features-based analytics run in parallel with, or complement, the use of established rule-based lexicons.

Necessity or nice to have? AI may not be fit for purpose across all communication channels, internal platforms or teams and activities. Whilst technological advancements are rapidly evolving, knowing when to adopt large language models (LLMs) and cloud-based solutions in communications surveillance is a question of risk appetite and prioritisation.

AI adoption drivers are more likely to be internal (drives for resource optimisation) than external (as a result of regulatory scrutiny). Potential internal strategic drivers include:

- **Effectiveness:** investing in AI and machine learning to improve surveillance results and reduce false positives
- **Efficiency:** increasing the scope and quality of surveillance coverage within an existing budget
- **Long term cost reduction:** investing in surveillance systems to ultimately reduce spend

Regulatory insight: Efforts to partner with industry and technology firms, such as the FCA's partnership with the AI Lab, show how regulators are pursuing a collaborative strategy to understand AI impacts. At present, attention is more generally targeted at markets and trade surveillance than communications surveillance, addressing questions such as the use of kill switches in the event of rogue AI trading. However, the ongoing regulatory focus on off-channel communications, in particular the large fines issued by US regulators for WhatsApp record-keeping failures, has resulted in significant upgrades to a number of firms' communication surveillance tools and programmes.

Four challenges to AI adoption

01 **Explainability:** a key challenge to AI adoption is how to explain the 'black box' thinking that supports generative AI models, particularly when the model is developed by a third party vendor. Whilst regulators and legislators push for explainability, there is a lack of consensus and regulatory guidance as to what this is means operationally, and in particular for surveillance activities.

AI technologies can explain their chain of reasoning, effectively 'showing their workings' on demand. This functionality can be calibrated to embed an explanation of the risk drivers and reasoning behind why a communication triggered a surveillance alert - and importantly, why it did not. This can also help identify and control for bias in AI thinking.

02 **Solving for data:** quality data and metadata, data pipelines and data governance must be in place to build AI infrastructure, and this relies on culture that accepts and recognises good data habits. AI will amplify weaknesses in data governance foundations, and there is broad recognition that there is still work to do.

Use of AI to improve end to end control frameworks and to upgrade record-keeping is premature, due to widespread needs to get the fundamentals of data governance, including meta data, tagging and cleaning, right, but in time AI is expected to mitigate data ingestion risks and identify blind spots in data governance, including data capture, data cleaning and data completeness, as discussed in the 2023 AFME paper, AI challenges and opportunities for compliance.

03 **Streamlining model risk management (MRM):** MRM is widely regarded as an essential, but bureaucratic machine that can fall prey to over-governance. One of the benefits of dynamic AI models is that the use of feedback loops to refine triggers and alert scenarios does not fundamentally change the model's architecture; this calibration is a retuning, rather than a retraining, of the model, which can result in more agile governance.

04 **Proof of concept (POC) pressures:** exploring POCs with prospective vendors means overcoming sizeable hurdles relating to data sharing, particularly data consolidation across multiple internal platforms. Together with data security, contract negotiations and internal governance, this often creates a material time lag, running the risk that obligations and technologies move materially before the POC concludes.

Two emerging questions

- Does the act of upgrading surveillance systems to use more complex technologies result in increased regulatory scrutiny, through introducing new operational and compliance risks?
- Surveillance is still largely isolated from other AI test cases; how do we encourage a move towards holistic data integration without undermining the importance of surveillance programmes?

www.thoughtnetworks.com