



**JOURNAL**  
**EDITION #27**

# **MARKET COLOUR ON E-COMMUNICATIONS SURVEILLANCE**

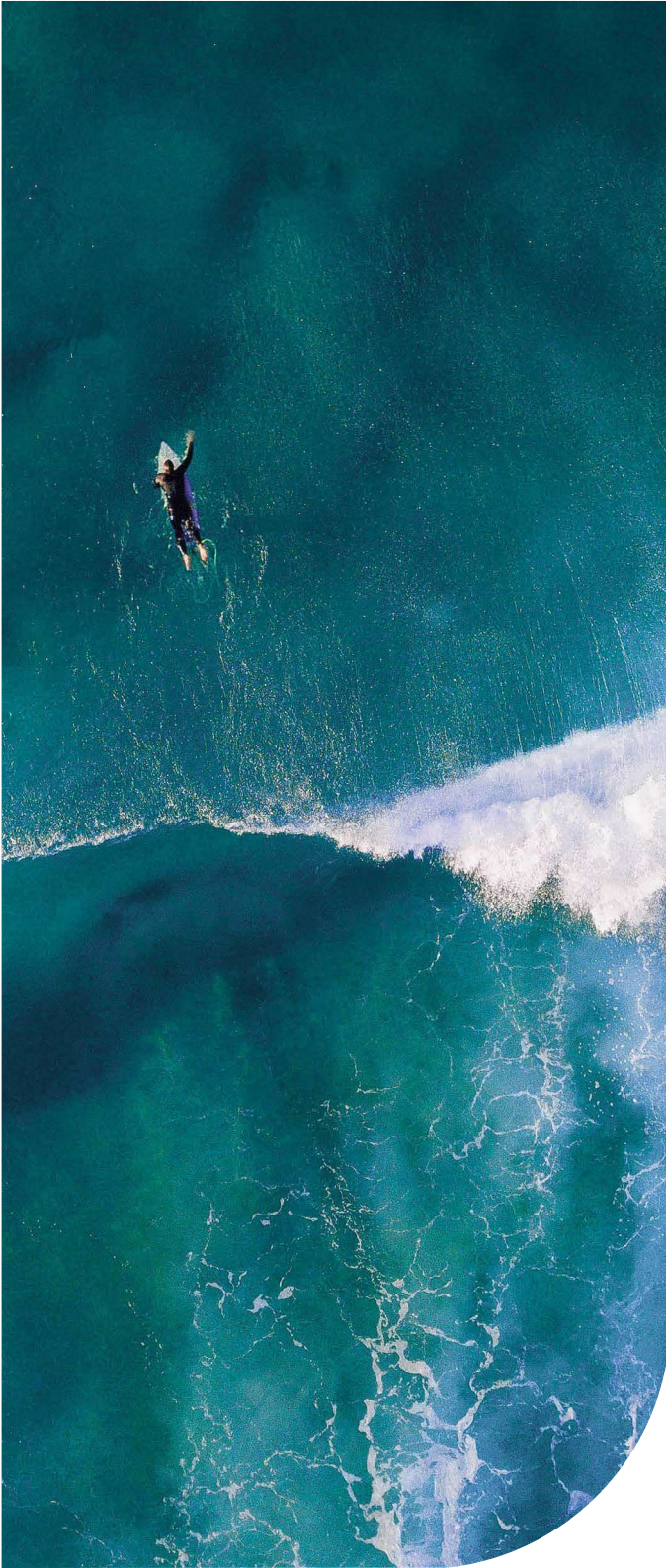
**BUILDING  
PERSONAL  
FINANCIAL  
FUTURES**

## EXECUTIVE SUMMARY

- Firms' communications surveillance capabilities are underperforming despite hefty investments in AI, machine learning, and voice analytics.
- Key issues facing monitoring programs:
  - Disappointment with AI/ML models missing critical risks
  - Outdated legacy voice surveillance tools requiring replacement
  - New voice-to-text tools struggling with costs and poor non-English accuracy
  - Testing reveals solutions hugely underperforming marketed capabilities
  - Overwhelmed compliance teams lack resources for expanded scope
- The findings highlight major technological gaps, operational barriers, and resource constraints impeding comprehensive communications oversight.
- As regulatory scrutiny intensifies expectations, firms face pressure to achieve compliant surveillance. However, significant hurdles remain in this industry-wide capability transition.





An aerial photograph of a person surfing on a wave. The surfer is a small figure in the distance, riding a white wave against a deep blue ocean. The image is partially cut off on the right side.

Electronic communications surveillance is a critical compliance function for financial institutions, helping them monitor employee communications for potential misconduct or regulatory breaches. Given the very real risks of fines, coupled with the reputational damage from oversight failures, implementing effective monitoring capabilities is an existential priority for firms operating in today's stringent regulatory climate.

However, our recent market research reveals that many financial institutions are struggling with the current state of surveillance technology and tools available. Despite investments in advanced systems powered by AI and machine learning, voice analytics and other cutting-edge capabilities, the solutions are not yet delivering what the practitioners say they need.

The research, which involved interviews with compliance leaders at 15 global and regional banks, uncovered several key findings:

**1. Dissatisfaction with AI/ML models:**

Practitioners expressed growing frustration that the AI and machine learning models used in many surveillance tools have not delivered the expected benefits. At least not yet. While these models can reduce alert volumes to some degree, they often fail to identify all the risks they are designed to detect, leaving compliance risks undetected. Part of the issue lies in unrealized expectations set by vendors overselling AI/ML capabilities. Financial firms were led to believe implementing these advanced technologies would provide a comprehensive solution for sifting through

massive data sets to pinpoint risk areas. However, the reality in practice is quite different.

**2. Legacy voice surveillance tools falling short:**

Many institutions still rely on older, phonics-based voice surveillance tools that are now broadly viewed as outdated and ill-equipped to handle modern coms-surveillance needs. To address this technology gap, many are looking to move towards voice-to-text (V2T) transcription tools as the next step, but are facing significant challenges with the cost of this move as well as concerns about the quality and accuracy of the technology currently available.

**3. Non-English Language accuracy issues with V2T:**

Those experimenting with V2T transcription tools are reporting poor translation accuracy. One bank using a market-leading transcription plus translation vendor said they were achieving around 80% accuracy for English but only 60% for Japanese. This low accuracy is observed across a range of non-English languages, both Asian and Latin-based languages were referenced, and is leading many to hold off on widespread deployment.



#### 4. **Resource-intensive testing and deployment:**

Moving to new surveillance tools requires rigorous testing and quality assurance before operational deployment can be approved. Institutions face significant hurdles in performing this testing, often lacking the resources and technical support needed to do so thoroughly. Testing can be time and labour-intensive, and several practitioners cited that after an intensive multi-month POC process, results were so disappointing compared to marketing promises that they chose not to deploy at all, post-trial.

#### 5. **Stretched compliance teams:**

Compounding the technical and operational hurdles already referenced, most participants raised concerns about bandwidth and their ability to 'keep up': static budgets, headcount pressure alongside

growing regulatory expectations and scrutiny is leaving many compliance teams struggling to manage the increasing volume and complexity of communications channels they need to monitor. This has left many teams feeling overwhelmed and under-resourced. Several commented that this imbalance between expanding channels and regulatory focus, against current resourcing and funding, is unsustainable.

The findings paint a picture of an industry function in transition, with institutions seeking to modernise their electronic communications surveillance capabilities but facing technological, organisational, and resource barriers along the way. Overcoming these hurdles will be crucial to ensuring effective surveillance and compliance.

**EMILY WRIGHT,**  
Consultant,  
Leaman Crellin  
[ew@leamancrellin.co.uk](mailto:ew@leamancrellin.co.uk)