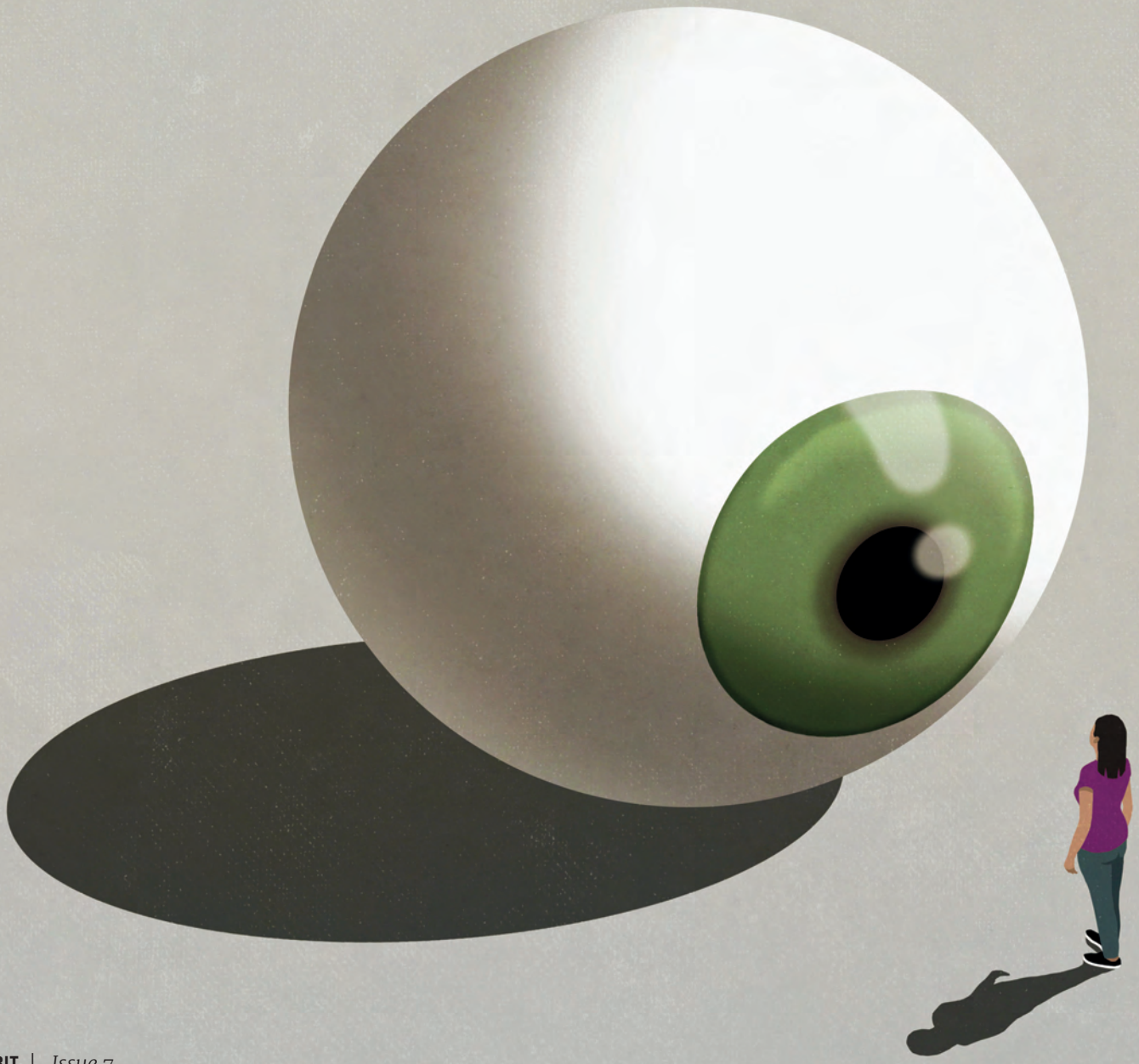
Trends in SURVEILLANCE

Even the established compliance practice of monitoring an array of data types for regulatory breaches and other forms of misconduct has evolved post-pandemic. But how exactly is the market changing, what are the key trends and where is surveillance practice heading?

Words by
ALEX VIALL



Speak to the experts on the frontline of surveillance and compliance and they point to a marked shift in practice in recent years, notably driven by a post-pandemic reset.

One surveillance practitioner *Orbit* spoke to anonymously, who has been at the frontline of this discipline for more than 20 years and currently works for a large global investment bank, sets the scene in a tier 1 bank: "Surveillance stalled somewhat during the pandemic," he explains. "Alert numbers went off the charts, as people were distracted and not as productive. Now we are just about back into the development cycle.

"A lot of the focus now is on coverage of areas like fixed income and exotics and getting that data into surveillance, but also asking what do you do with it once it is there."

Intense focus

He is absolutely convinced that we are moving into a distinctly new period.

"I have never seen regulators as interested in surveillance as they are currently," he says. "The focus is intense. This is because it has always been the poor relation to advisory, and this is just banks reaping what they sow.

"Surveillance is expensive to do well. The banks have tried to cut cost on the human resource to make up for what they pay for technology.

"It has led to a problem with making challenges and I think that the credibility and standing of surveillance in banks has got lower and lower. Regulators have twigged this and realized what an important component of compliance it is, and that this is probably the best place to gauge corporate culture.

"This focus has been a long time coming and is all happening at once – it is a global phenomenon and not regional.

Fragmented approach

Summing up where the trade side is headed, he tells *Orbit*: "There is fragmentation that we have not seen for a while. You used to have to buy SMARTS and do bits around the edge but there is no obvious vendor so many banks are going DIY, which might mean we get very different levels of surveillance that could lead to some positive reinforcement.

"This is where one bank identifies something and then the regulator goes to another and asks why they cannot identify the same thing. We have missed this sort of feedback in the fixed income and non-equity space."

Behavioral alerts

He continues: "We are also leaning towards behavioral alerts, too. But the balance is always between explainability/reliability versus innovation, and they are not aversive. But baby steps is the right approach here. We cannot go all in on AI overnight as we want to get every step right as we go along.

"We are lucky to have our very own real examples of spoofing we can train our data on. But this means some banks have different experience and sight and data – the tier 2s might not even have the data to train their models."

For Aaron Stowell, Director of Forensic Technology and Surveillance at KPMG, the key is convergence. He explains: "Convergence is taking place at the software level but no one has cracked it. The search for a holistic solution continues, and so right now it requires manually wiring everything together.

Better tuning

"There are some trading risks that require better tuning that are not well represented in existing rules or models," »

> *"The focus is intense. This is because surveillance has always been the poor relation to advisory, and this is just banks reaping what they sow"*

Stowell continues. "If you have never traded a particular asset before then you are going to get outliers, and that leads to some firms performing analysis in Excel spreadsheets and custom systems.

"The real innovation is allowing firms to build those rules quickly to import them into their trade surveillance system so it is all in one place, and the platform that allows you to do that will be the one that wins out."

I ask Stowell whether he has noticed any regulatory interest in voice and other data types and his answer provides a stark warning: "I have not seen regulatory focus to be so high – it is the detail of the questions, and what they expect us to find that is eye-watering. So now we face the reality that we are going to have to do stuff with trade and voice and comms that we were not doing previously.

"It is also about understanding where the issues are. The latest WhatsApp fines are interesting as what was made really clear is that it was a recordkeeping breach. In surveillance a lot of our problems come from bad data when we actually don't have the opportunity to do surveillance as we don't retain the data. That is not a surveillance issue – we need to be senior enough to make that challenge to the front office.

"The regulators are actually doing us a favor even though it might not feel like it when the enforcement strikes! But projects that had been on the backburner for some time are now coming to the fore – such as voice – and part of this might be due to the new hybrid work environment as a catalyst.

"But we had it on our to do list, plus with regulatory clouds darkening and new tech available the timing is right."

Holistic approach

I want to find out if either of our experts thought the prospect of carrying out holistic or integrated surveillance is any closer. Our surveillance practitioner has this to say. "Regarding the quest for a holistic solution, senior management and compliance want big wins quickly and some of the basics are not sexy but they are necessary.

"The start of doing holistic is actually doing case management properly and most banks are shockingly bad at this in surveillance. This, along with bad data handling, means there is siloed work with no standards.

"We are finally bringing everything together, tracking what we have to do, standardizing the data and we now have a closure rating matrix as a standard to bring out the risk from alerting, which is step one of holistic. Most places don't have it all in one place – they have to go to 10 systems to get the full picture. Bringing the alerts together is quite profound as you do spot stuff you could not have identified."

Structure and tradition

He continues: "Step two is the structure of the surveillance teams. I am not convinced that having a comms team and a trade team standing alone is the right structure. But that is tradition. Equities and fixed income might be a better approach, where one team looks at comms and trade together for that asset class.

"The offshore setups in many banks also hinder this. It is a slow burn as some bad structural habits persist that are beyond pure tech here."

Few readers will need reminding that enforcement issues around the use of personal devices is a particularly hot topic right now. Our surveillance practitioner provides an inside view: "It is very difficult still as we have the view that if someone wants to subvert the system and communicate on unrecorded channels they will, whatever the controls you have in place.

> *"I am not convinced that having a comms team and a trade team standing alone is the right structure. But that is tradition. Equities and fixed income might be better"*

Change expectations

"We have not been clear enough historically about our expectations and so there has always been an allowable gray area where if what you are doing is not business related you can use WhatsApp. This leads to other things though, even if the originating message or engagement was not about business," he continues.

"We look at change of venue surveillance and when we challenge people we find that by message 50 there is pricing and it is clearly business content in there. It happens. We need to change that expectation and so now, without exception, it is forbidden for you to have any contact with your clients on WhatsApp.

"This is step one and a short-term fix as we are trying to hold back the tide – banks actually banned the use of email when it first came out, which sounds appealing now.

"We never went BYOD but it was clear the devices we supplied were crap, so we heard the complaints and now we make them more appealing, with upgrades to new iPhones with better software and improved Office365 and ways to enable WhatsApp and WeChat via a Symphony connector, even though they are not very good long-term fixes. We are experimenting.

Bye bye BYOD

"It has killed the tech team's quest to go BYOD forever. We make the work device usable so there is no excuse or gray area. So if we investigate change of venue and we find people using a personal device there is no excuse – this is a culture change and a move we are making. The US regulations are extraterritorial and they sit very uncomfortably with GDPR as privacy has not got teeth in the US like in the EU. The broader ethical point around mass surveillance is also somewhat oppressive.

Stowell adds: "It comes down to the culture of the organization and many used to ban the use of personal devices on the trading floor. Others felt that practice was bordering on inhumane, and people

If someone wants to subvert the system and communicate on unrecorded channels they will, whatever controls you have in place to prevent it"

need to get in touch with families in an emergency, so more leeway was allowed.

"Since the WFH environment kicked in, that has made everything harder. There is often a disconnect between the investment bank and group technology teams, but these new comms channels need to be assessed, approved and onboarded at deal speed – not two years later for WhatsApp, people are already using it. The time lag between initial use and capture is inevitably going to exist.

"However, people are only doing basic reconciliation, and most are not running effective rules or models to pick up venue change. Very few are taking advantage of what is possible, linking email signatures to mobile numbers and cross-referencing call logs to see which mobile devices are being used.

"Then there is aggregate analytics for traders and desks, so for trades being conducted you can do basic trade reconstruction for Dodd-Frank in 72 hours. Most are doing this manually and it is a hard problem to solve. If you have a trade and you cannot match that to a recorded comm you have an issue. That is the forefront – that is the expectation."

Is it likely that SMCR would kick in here around enforcement actions? Our surveillance practitioner warns: "The FCA has hinted that a review of business comms use is coming.

"SMCR has had a lot of impact despite no actual cases getting headlines – everyone is very scared so it has been a deterrent. Banks are often allowed to deal with the issues first and if FCA disagrees then they step in. But it does not look great – being fired seems reasonable punishment here.

"It is a missed opportunity for FCA if they don't use it, as for it to remain as something to be feared and respected, they need some precedent. Juniors on a desk cannot be blamed for following suit if their manager or supervisor is merrily using WhatsApp. Culture comes from the top.

Stowell adds: 'Why have the regulation if you are not going to use it? Now is the moment as there were some egregious instances. I am not sure when but I would be astonished if it does not happen. The indication is that one of the traders contacted their broker and encouraged them to delete the messages, suggesting a move to Signal which is encrypted. This is really unbelievable behaviour, and the fines reflect this. It suggests more must come.' ●

IMAGES: GETTY