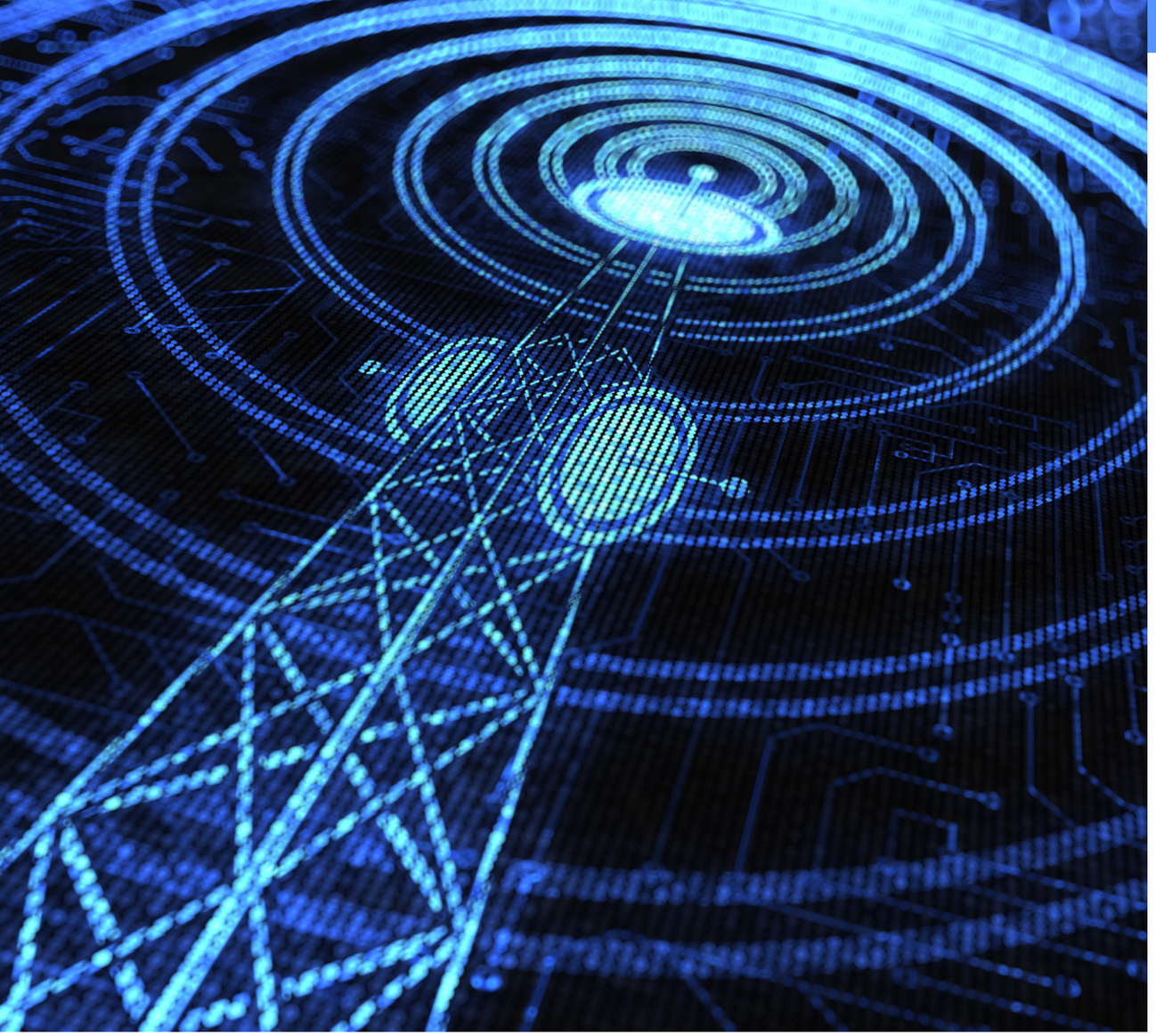
VOICE SURVEILLANCE FORECAST 2022

smarsh® | 1LoD®



Raising the bar in surveillance

Key Takeaways

- Retention of required communications, including voice, is now a serious regulatory focus
- Policies alone are no longer enough: regulators want evidence of implementation
- 71% of banks think their investment in surveillance is sufficient
- But a majority rely upon voice surveillance techniques which they consider to be insufficient
- 81% of banks admit their trade and comms surveillance integration is a work in progress
- Vendor integration issues make one-stop compromises attractive
- Random sampling has no place in an effective voice surveillance process
- Machine learning is increasingly important in improving core voice processes

> *"There has to be a culture of compliance. Training is not enough. Attestation is not enough. Compliance with these recordkeeping requirements is so technologically difficult that it goes far beyond the responsibilities and power of the compliance department to ensure that it is carried out. Everyone is in charge of complying with the federal securities laws."*
>
> - THOMAS P. SMITH, JR., ASSISTANT REGIONAL DIRECTOR,
> NEW YORK REGIONAL OFFICE, US SECURITIES AND EXCHANGE COMMISSION

The need for next-generation voice surveillance programmes is becoming ever more urgent. A recent, significant enforcement against J.P. Morgan Securities and a more transparent regulatory stance have shown the importance of getting this right, particularly at a time of increasing cost pressures and advances in technology. Yet many banks have barely begun to address the issue.

Surveillance professionals gathered in London in March to discuss the latest developments in voice surveillance including regulatory enforcement, the integration of voice with e-comms and trade and a range of other technology issues. This Deep Dive follows a landmark SEC ruling against J.P. Morgan Securities in December 2021 when the bank was fined a total of $200 million for failing to keep records of the personal emails, text and WhatsApp messages sent by its employees and even their most senior supervisors. The case showed the critical importance of capturing all of the communications of regulated individuals, regardless of channel or how difficult that task is.

Thomas P. Smith, Jr., Assistant Regional Director, New York Regional Office, US Securities and Exchange Commission, opened the event, setting out the main takeaways from the ruling and associated fine for financial institutions.

First, regulations concerning the retention of records are clear and broad: all communications related to the business, with clients or between colleagues, must be retained so that they can be submitted to regulators if required. Banks therefore have no choice but to work out how to retain texts, chats, voice recordings, and messaging embedded in collaboration or trading tools and in video. This is not optional.

Second, having policies in place is not enough. Policies must be implemented and that must be provable. In the J.P. Morgan case, the regulator pointed out that there was a widespread failure to implement written policies and that supervisors themselves routinely ignored those policies and used prohibited messaging apps and other channels. This lack of a correct tone at the top was noted and the ruling included a charge of failure to supervise which explicitly recognised the fact that senior supervisors at the firm did not ensure that securities laws were followed.

And finally, Smith said, there has to be a culture of compliance. Training is not enough. Attestation is not enough. Compliance with these record-keeping requirements is so technologically difficult that it goes far beyond the responsibilities and power of the compliance department to ensure that it is carried out. Everyone is in charge of complying with the federal securities laws.

Spend, spend, spend?

These regulatory expectations, and the size of the penalties for failing to meet them, significantly raise the bar for surveillance professionals, supervisors and senior management. None of the challenges are new, but the fact that no leeway is given for non-compliance is a game changer. As one attendee said, “This [voice and multi-channel surveillance] is an area that has become exponentially more difficult to comply with. It’s an area that requires investment, and [the ruling is] actually a verification that regulators are taking this seriously. From here on in, I think it’s very clear. You have to look at all channels all the time – and are you up to snuff with them?”

So, what does this mean in practice?

First, it puts the emphasis back on capture and archiving. As one attendee put it, “You can have the best surveillance system in the world – you can spend an absolute fortune on it, but if the bank hasn’t invested in the underlying infrastructure and kept up with technology, your surveillance system is completely useless.”

This, in turn, means identifying which platforms employees are using; in many cases this also requires more work, often with vendors, in understanding the functionality of those platforms and whether they can be captured (web portals in fixed income are a current worry for the FCA, for example). Given the proliferation of communications and trading channels, this is becoming increasingly difficult. Second, it implies additional investment or a better use of current resources may be required. If banks’ current investment levels have not solved these problems, then do they have to spend more? Perhaps surprisingly, in a poll of the attendees, 71% said they believe their firm is investing in the surveillance function sufficiently to meet regulatory expectations [chart 1].

That said, participants agreed that this investment does not preclude the need to continue to invest in keeping up with technology, new communication mechanisms and the global challenge of integrating them into legacy frameworks. They also pointed out that if banks cannot afford the infrastructure required to comply, then they need to work harder at cost-effectiveness. Minimising costs and addressing the huge inefficiencies of most alerting processes is one way to do that. But there is also increasing recognition that the affordability of surveillance compliance will depend on maximising the value of the data collected.

As Dr. Michael McGrath, Senior Director, Archiving, Compliance and Digital Risk, Proofpoint, explains: “On the one hand, it is going to be essential to have a unified approach to capture, archiving and surveillance and in particular having one copy of the data in one place and normalizing it so that you can apply the same controls and analytics to it, so that you are not repeating processes across separate platforms and you can start to drive efficiencies in terms of accuracy and speed. But on the other hand, banks also need to find ways of maximizing the value from the data. This is really valuable data. Used properly it can generate significant P&L for the business. Getting that message across is a key part of the affordability argument.”

"As for voice and e-comms, yes, we’re going through a journey to properly link them together, but I think we all agree that there have been tremendous gains in accuracy in voice-to-text over the last year to 18 months and that is paving the way to making that larger integration between trade and comms possible."

JOHN HOLLAND, SENIOR VICE PRESIDENT, SMARSH

Integrating trade and comms

Integrating surveillance silos is another way to increase both the efficiency and effectiveness of surveillance programmes. The unification of trade, e-comms and voice surveillance has long been seen as way to solve both cost and effectiveness problems. But is it feasible?

For a start, have banks even managed to integrate voice and e-comms surveillance? When attendees were asked, ‘How successfully is your voice surveillance programme integrated with other surveillance channels?’, the overwhelming majority admitted that this was a work in progress – which in reality means not much has been achieved.

Technologists are certain that the voice/e-comms piece of the jigsaw is being solved. “As for voice and e-comms, yes, we’re going through a journey to properly link them together, but I think we all agree that there have been tremendous gains in accuracy in voice-to-text over the last year to 18 months and that is paving the way to making that larger integration between trade and comms possible,” says John Holland, Senior Vice President, Smarsh.

Attendees were also optimistic about broader comms and trade integration. When asked, ‘Is the comprehensive integration of communication and trade surveillance data a realistic technological possibility?’, 74% said that it was [chart 3].

However, it also depends on how you define integration, and on the time frames used. True integration was seen as a process in which trade data and communications (voice and e-comms) data are ingested effectively in parallel and then linked so that all the data relating to a specific transaction are available at the click of a button on one dashboard.

One head of surveillance described this scenario as “a kind of Nirvana state,” and said that achieving this would be “extremely hard.” He added: “It’s not just an engineering challenge, it’s also an organisational maturity challenge, because you need to have things like your records management policies and processes really closely coupled with everything that the firm is doing, and you would need very, very strong engagement with the 1st line to even think about attempting to do that. I’ve never seen that done at scale outside very limited POCs.”

CHART 1

I think my firm is investing in the surveillance function sufficiently to meet regulatroy expectations:

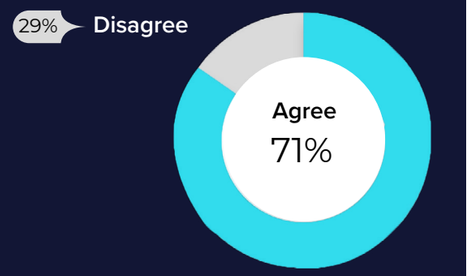


CHART 2

How successfully is your voice surveillance programme integrated with other surveillance channels?

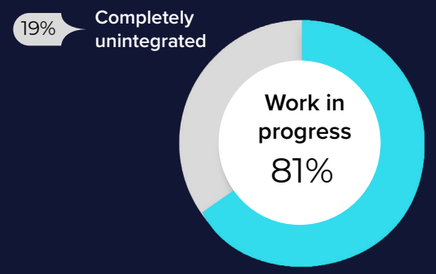
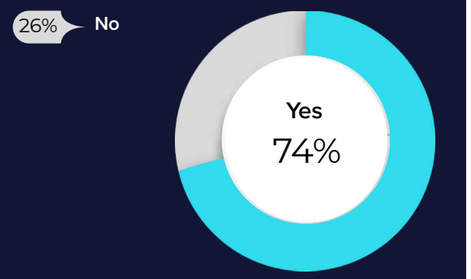


CHART 3

Is the comprehensive integration of communication and trade surveillance data a realistic technological possibility?



With an alternative, more limited form of integration, surveillance is viewed as a downstream function which takes comms data into its comms programme and trade data into its trade programme and analyses them separately, but then integrates the outcomes from the two processes. “If the poll respondents mean the latter, then I would completely agree with the result,” this head of surveillance said.

Some banks and vendors are working on variations of the downstream idea. Comms data and/or metadata is fed alongside trade data with relevant matches highlighted on the basis of the time at which trades and calls/emails occurred, or, in smarter solutions, on the basis of content matches between, say, the name of a traded instrument and a keyword picked up in the comms data. This gives analysts or investigators faster access to the comms context in which a trade was made, allowing true positives to be identified more quickly and escalated where necessary, and for false positives to be closed out.

Others see the case management system as the starting point for trade/comms integration. Whether this implies the existence of a single upstream surveillance data lake or whether the downstream alert feeds are the source for an integrated case manager was a matter of debate, but there was agreement that “You can get quite a long way on that journey of integrating comms and trade with a well-constructed case management system. And that can either be built in-house or there are a number of good vendor solutions outside as well.”

The latter types of solution are seen by some as an answer to the potential cost implications of full data integration: costs. As one participant put it, “There has been a staggering investment by banks to get surveillance working to the point we are at today. So, we do have to think about what’s the incremental benefit of a full-scale technical integration, as opposed to more light touch methods which I think would be available and usable by a broader range of banks. There’s a big gulf between what the top 10 banks spend on their solutions and what the mid-size banks spend on theirs. So, I would suggest there are other ways to use existing technology, to maybe get quite close to this integration, and give technology and the really good vendor solutions that are being developed right now a bit more time to mature."

Vendor collaboration challenge

When thinking about these types of projects, it’s easy to focus on the in-house systems, data and organisational aspects of integration. But a key additional complication is the integration of disparate third-party vendor technologies, both legacy and new.

As one surveillance lead explained, “I think about integration in two distinct ways. There is the desired outcome – how do we integrate the outputs, in this case, of voice, into our existing framework to create more holistic surveillance of a set of alerts or, more broadly, employee behaviour? But before that comes the technical integration – how do we integrate third-party vendor solutions into our existing infrastructure?”

That technology integration is critical, particularly in the case of voice, because banks so often use separate vendors for capture, archiving and transcription, with additional suppliers for the transcription and translation of additional languages. Those solutions then need to connect with what is usually an existing e-comms solution.

This raises a number of questions: instead of trying to integrate vendor systems, is it better simply to compromise and buy a single system that can satisfy most of your objectives? As one attendee put it, “I think up front you really need to consider if there’s a vendor that has one product and is willing to work with you on developing additional features that you need. You need to look at the cost/benefit of that choice.”

If the decision is made to go with multiple vendors, then it may be sensible to bed one solution in first before moving onto others. This means starting by solving one problem, say e-comms, and then moving on to voice. As one bank discovered, this approach can pay off unexpectedly: the first vendor developed additional capabilities while implementing the initial solution. By the time the e-comms project was complete, the vendor had developed a voice solution which meant that the bank did not need to go through the procurement and development process required to bring another supplier on board.

It is also crucial that vendors are willing and able to work together and, potentially, change their offerings to suit each other’s technology. And finally, many participants stressed the importance of establishing a common understanding and vocabulary. “We struggled to make our vision and requirements clear to one vendor because it turned out that we could not use the terminology from our existing surveillance systems to this vendor because they would call things a bit differently. So, we often found ourselves thinking that we understood each other, when we did not. That has been a painful learning curve for me in the implementation phase,” explained one European surveillance chief.

The vendors agree with this and some even go further. It’s not simply important to be able to integrate with other vendors: it’s critical, if banks are to start building more proactive surveillance compliance systems, for technology providers to connect with all of the different systems that come together in the surveillance compliance function.

As Phil Fry, Vice President – Financial Compliance Strategy, Verint, explains, “Vendors absolutely need to understand the clients’ end-to-end surveillance lifecycle and their requirements and the language they use. They absolutely need to be able to work across technologies, and to provide open APIs to facilitate that. But they also need to be able to partner with everything from critical front-end functions to core capture technologies to sophisticated analytics and policy management automation systems. Looking for suppliers who can do that, and who do offer more than single point solution to one problem is the right route for many institutions.”

This raises an important question: instead of trying to integrate vendor systems, is it better simply to compromise and buy a single system that can satisfy most of your objectives?

CHART 4

Sampling plays a significant role in our voice surveillance programmes:

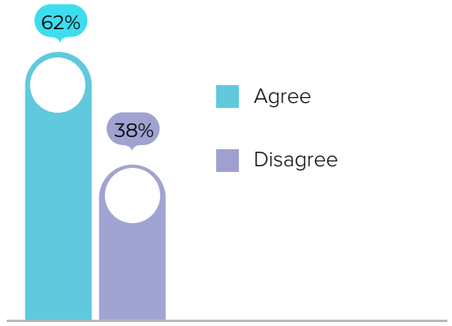


CHART 5

Is random sampling still part of your voice surveillance programme?

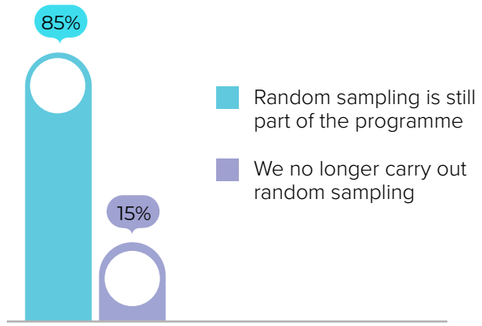
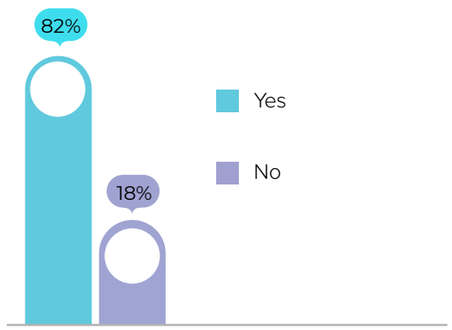


CHART 6

Is random sampling of voice surveillance sufficient?



The many faces of sampling

Asked whether sampling plays a significant role in their voice surveillance programmes, 62% of attendees said that it did [chart 4]. But what did they mean?

In the simplest form of sampling, surveillance teams sample a small, random subset of monitored individuals per month against a fixed lexicon per language. The size of the samples is dictated simply by the banks' capacity to analyse – subject to the relevant regulatory minima. "We are just going to sample a random selection of calls and listen to them because the technology is not there to run a more programmatic surveillance process," as one practitioner put it.

The limitations are obvious: if you only sample a small percentage of the communications of a small percentage of the required population, it is very likely that instances of misconduct will slip through. This is why even those (many) institutions still using this approach do not believe, as one participant put it, "that this particular type of random sampling has a future in mature surveillance. It is where we are currently, but we are moving to a more automated surveillance programme."

This bank is by no means alone. Asked whether random sampling was still part of their voice surveillance programme, 85% of banks said that it was [chart 5].

And asked, 'Is random sampling of voice surveillance sufficient?', 82% said that it was not [chart 6].

Next-level sampling

Automation enables larger percentages of populations' communications to be monitored and analysed, theoretically leading to lower levels of sampling. However, that assumes that lexicons, transcription of voice to text, phonetic lexicons and all the tools used to parse voice communications are themselves good enough to identify all the misconduct potentially contained in the comms. None of these assumptions is true.

To fix that problem, a different sampling paradigm is needed. Next-level sampling applies machine learning (ML) to the existing automated process to create a more sophisticated filter. Machine learning can be applied at multiple points in the process. It can be applied to transcription to make it more accurate; it can be used to help categorise calls which can help with assigning risk to each call category (e.g., analysts calls, personal calls, calls where ML detects trading activity, etc.); it can be used in risk detection models.

However, because none of these processes are totally reliable, and in particular because real-world, voice-to-text transcription accuracy is still unsatisfactory, sampling is still critical. In this context, though, it now means something different: how to find the relevant calls and the relevant section of calls for people to listen to. It is not used to arbitrarily reduce the set of analysed calls to a number that a particular bank's monitoring processes can handle; it is used to locate the calls most likely to contain material that should be analysed. This still leaves most communications unanalysed, but the selection is now risk-based rather than random.

As Jordan Domash, General Manager, Relativity Trace explains, "The way we think of it is that the analyst will have to listen to a call at some point. So, how do you get to the call and the part of the call you need in the least time? One way is to build the dictionary, the custom words, acronyms and phrases that match your business and risks, and generate a transcript. The ML is then trained to find not just those words and phrases, but also things like them, even if it only has, say, a 50% confidence that it has identified it correctly. This in a sense expands your potential false positives to get a wider capture but only around a very specific set of risk-based criteria." This is still sampling, but at a different level of sophistication.

Most banks are not there yet. Asked to rate their firm's level of maturity in using machine learning to reduce voice surveillance false positives on a scale of 1 to 5, with 5 indicating that they had not started the journey, 60% rated themselves 4 or 5 [chart 7].

Sampling for QA/UAT

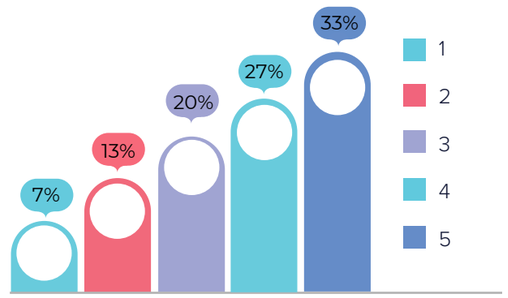
No matter how sophisticated a voice surveillance process is, it still needs to be assured. As one attendee pointed out, "The more technology you apply to any sort of solution to create efficiencies, the greater the need to make sure that technology continues to operate as you'd intended when you deployed it. We have invested a lot of time and effort in creating technology to improve our surveillance programme. But we do have to periodically go and validate to make sure that it does indeed do what it says it does."

That quality assurance, or user acceptance testing, is carried out through sampling. In order to assure themselves and the regulators that automation and risk-based sampling work, institutions will continue to evaluate what they would expect to find in the output of their voice surveillance process versus that which is shown to be within the system as a whole by a broader sampling process.

It may seem ironic that sampling is deemed so inefficient and ineffective in identifying market abuse that it has to be replaced with automation and smart technology, but it is still the preferred tool for assuring that new technology works as expected. That is perhaps the final reason why so many attendees said that it still plays a significant role in their voice surveillance programmes.

CHART 7

My firm's level of maturity in using machine learning to reduce voice surveillance false positives is: 1: High (Mature and fully embedded in our voice capability) to 5:



This information was taken from the Voice Surveillance Deep Dive 9 & 10 March 2022.

For more information on 1LoD please visit: www.1lod.com