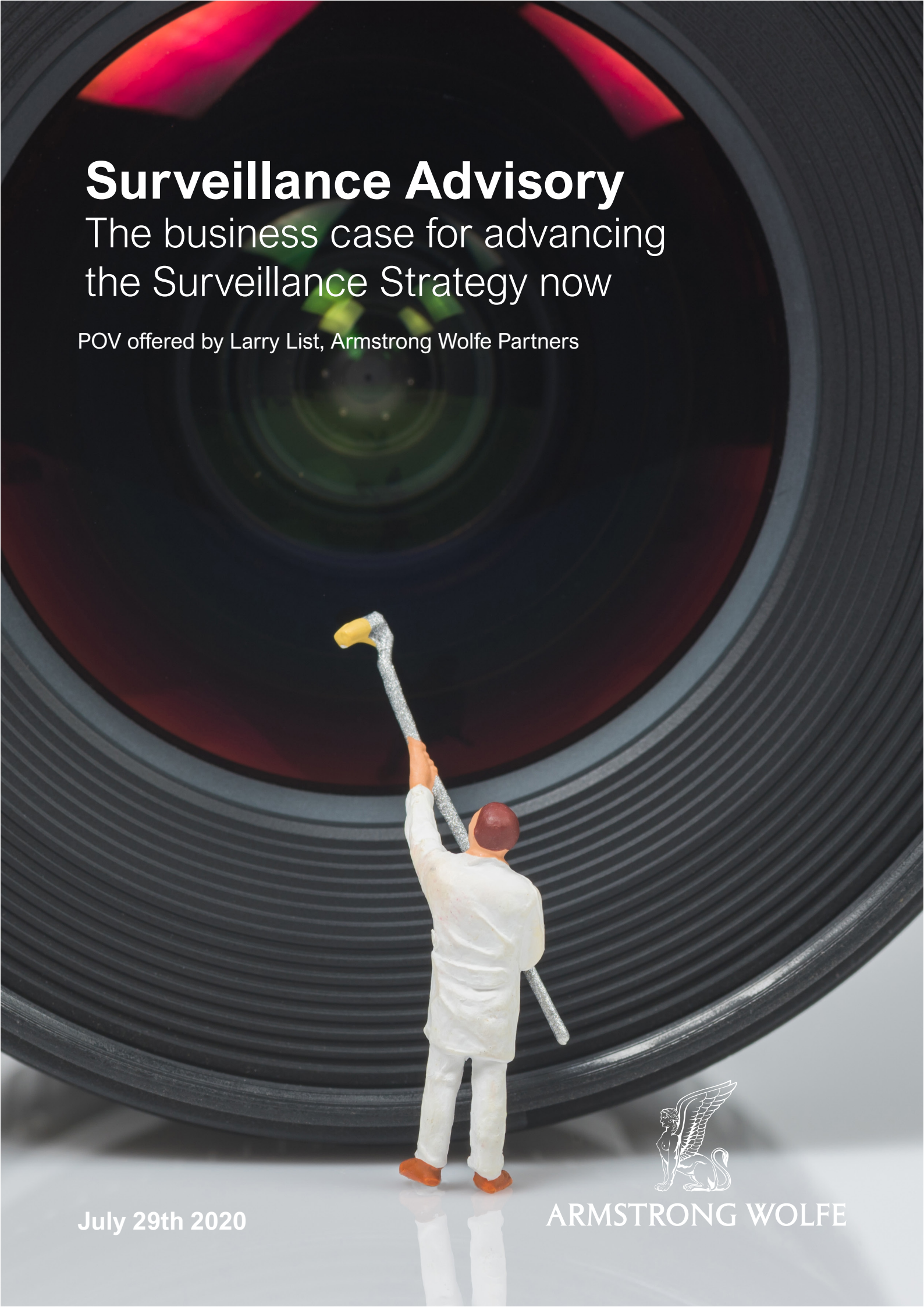
Surveillance Advisory

The business case for advancing the Surveillance Strategy now

POV offered by Larry List, Armstrong Wolfe Partners



July 29th 2020

ARMSTRONG WOLFE

The business case for advancing the Surveillance Strategy now

> *…this call is being recorded for quality control purposes*

> *…don't worry about the 'beep' you hear - it is required to let you know the call is recorded*

We have become used to these messages as standard operating procedure. But for various reasons institutional financial services businesses have not yet adopted automated voice surveillance and the risk management advantages it provides. Why are calls being recorded in the first place, but then not surveilled? Verbal interactions (internally and externally) are still key to markets and banking businesses, and now remote working and associated risks become the main drivers.

A minimalist set of regulatory and legal requirements, combined with a developing technology landscape, have resulted in passive approaches to voice surveillance. Firms will take some comfort in a sampling approach, one-off trade reconstruction exercises, and also accessing recordings for playback if a specific issue arises, such as addressing client complaints. This is a reactionary set of processes, and unlikely to be able to meet the conduct risk management challenges going forward.

Considering the topics of written electronic communications and trades surveillance, regulations are clearer as FINRA, the CFTC, and the UK/EU (via Mfid/MAR), have more precisely defined the surveillance and retention requirements. But even with these rule-sets, firms have implemented a wide range and depth of surveillance strategies, under the umbrella of being "risk-based". Generally, the approaches deployed remain aimed at the core regulatory requirements in the first instance, and addressing specific supervisory needs follow, but usually fall short due to lack of budget. In fact, most firms are increasing the cost pressure on surveillance functions as remediation programs wind down and BAU takes over.

Lastly, the overall effectiveness of the surveillance frameworks in operation varies greatly across the industry. In many cases, the data is simply not well-structured to allow for efficient processing. With too much noise generated via excessive, low risk alerts, little management benefit is realized. To add, older technology is ingrained into firm's overall IT eco-systems, dramatically inhibiting inter-operability and change/advancement opportunities.

Advanced technologies are now available in the market, but leveraging these technologies needs a clear commitment from Management to be successful, which up to now has only been supported marginally – committing a skilled user base to design and operate, developing clean data structures, and executing integration projects into the core IT eco-systems. Another headwind is that AI/Machine Learning models are not yet fully reconciled with regulatory acceptance, although this process is developing.

To the industry's credit, firms have effectively managed through the initial crisis, and surveillance functions have provided the "safety net" for identifying questionable market practices or behaviours. In general surveillance seems to have worked to Management's satisfaction, but it is too early to reflect on lessons learned as issues will likely be uncovered going forward.

The industry is at a key inflection point for surveillance and supervision. Regulatory and Governmental authorities are focused on how leaders are managing the new dimensions of risks and threats, as well as how conduct, control and all the non-financial risk management programs can continue to be effective in remote working. At the same time, there are increasing cost pressures on COOs, CCOs especially with any new proposals. Investments in conduct and control programs are increasingly requiring explicit commercial benefits and/or returns on investment to be approved.

What does seem clear at this point is that a dispersed workforce will continue for some time. Certain functions such as Trading may return to the office more quickly (Q1 2021?), but there is no doubt that key functions, including many which are client-facing, will remain remote. This raises the questions of what new tools, technologies and policies will be needed to work remotely in a safe, sustainable way, and how should the surveillance architecture adapt to the new risks and ways of working? Supervisors will ask themselves if their risk lens and tools are sufficiently wide and robust to detect emerging issues? How can surveillance be expanded to better understand patterns and cause/effects beyond traditional communications and trade surveillance?
And is it all worth the cost?

The business case for advancing the Surveillance Strategy now

The business case is clear. A progressive surveillance function is foundational to strong supervision and conduct programs, and has moved beyond specific regulatory rules compliance. In these volatile times, the surveillance strategy should be continuously evaluated to ensure it is risk-adjusted, relevant and sustainable. Key to this evaluation is also bringing commercial benefits and advanced risk management capabilities to the fore. From an investment perspective, it is likely that investing in advanced surveillance capabilities and developing these commercial opportunities, can be achieved through well-planned resource optimization and reallocations, with limited net spend increase in the short term, and likely cost savings in the medium term.

Supervision and Conduct Management is more complex and inter-connected than ever, especially with a remote workforce, and increased personal accountability. External threats are heightened, global recoveries will be uneven, market dislocations will continue, and performance pressures are increasing. An effective surveillance function leverages the supervisor to enable closer, proactive management of conduct and behaviours, as well as managing aspects such as new joiners and staff turnover. This proactivity enables a supervisor to take timely action and potentially head off problems before they escalate. Finally, well-developed surveillance creates evidence of supervision through the generation of MIS and metrics.

Shareholders need to be protected. Massive fines and operational losses have challenged shareholder confidence in Boards and Management in being able to supervise staff effectively, and eliminate collusive and fraudulent actions (codified through the SMR). Surveillance is a key, promoted response and demonstrates (in part) executive commitment to improved conduct, controls and non-financial risk management. To add, regional regulatory and legal rules across the globe will actively develop (i.e. the HK National Security Law and its potential extraterritorial impact), and strong surveillance capabilities are directly responsive to managing supervisory and conduct risks during these evolutions.

ROI and Client opportunities. One of the most pressing client concerns relates to confidential data protection. Client RFPs are more commonplace asking firms to document and continuously update its client protection mechanisms including surveillance for data leakage, inappropriate information sharing monitoring, and systems access controls. Customizing surveillance methods towards protecting client interests is accretive in building stronger relationships and developing more business. Surveillance also will add insight to communications and trading patterns. For client interactions, the topic of "communication density" is relevant, as firms are constantly optimizing client tiering and coverages. Surveillance can quickly provide a holistic analysis on communication trends, which can directly inform resource allocations. Another key area of surveillance that contributes to value creation/ preservation concerns data loss protections. Quickly identifying data breaches such as sending out client lists or proprietary code represents clear value preservation, allowing for fast reaction. Advanced fraud detection in the first line is also possible. Examples will include special monitoring of T&E, or the tracking of holidays/business trips/client events. Using AI in the 1LOD will further enhance pattern development for payments to help protect against anomalous or potentially fraudulent activities.

The good news is that designing and delivering an effective surveillance program is achievable, and can be implemented in a way that minimizes operational risks, allows for component inter-operability into a larger eco-system, and is customized in a risk-based fashion.

Armstrong Wolfe Partners understands the key components of a best-in-class surveillance and threat detection function, which allows for a rapid assessment of a firm's current capabilities, and then directly focus on actionable initiatives. A typical assessment would require 4-6 weeks depending upon the complexity of the current operating environment, and includes an industry benchmark to other programs. AWP closely collaborates with Management in each stage of the process and provides clear progress reporting throughout.

To get started please contact AWP for an initial discussion on surveillance and threat assessment, and see how AWP can add value to your strategy and execution.

Larry List
Armstrong Wolfe Partners
l.list@armstrongwolfe.com

For general enquiries, Executive Search, Career Management and Marketing please contact:
info@armstrongwolfe.com
Telephone +44 (0) 20 3664 8863

armstrongwolfe.com

Find us on LinkedIn

Armstrong Wolfe | Women in the COO Community | Global COO Community