Navigating strict privacy regulations in a MiFID II world

The Realization Group

shield.

Navigating strict privacy regulations in a MiFID II world

Recent regulations have obliged financial services companies to provide greater visibility into their operations. The European Union's Markets in Financial Instruments Directive II (MiFID II) and its UK sibling, the Markets Abuse Regulation (MAR), has encouraged the surveillance of all trading-related communications, both spoken and electronic (eComms), between employees, their clients and third parties.

However, the EU's General Data Protection Regulation (GDPR), enforced in the UK under the Privacy and Electronic Communications Regulation (PECR) and Data Protection Act (DPA), threaten huge penalties for the misuse of personal data. The surveillance and storage of communications-linked data will be given another layer of regulation under the EU's upcoming ePrivacy Regulation.

In this report, Mark McCord and Mike O'Hara of The Realization Group examine the seeming contradictions between these two sets of edicts. Along with **Anish Kalraiya** of Crédit Agricole CIB, **Adam Clarke** and **Balavernie Sritharan** of Deloitte, **Paul Clulow-Phillips** of Société Générale, **Sam Tyfield** from Shoosmiths and **Shiran Weitzman** of Shield they also discuss how compliance officers are dealing with this conundrum and consider emerging challenges to achieving compliance.

Compliance, Confusion and Contradiction

The first iteration of the financial industry's strict transparency code came into force in 2007 in order to harmonise rules governing transactions and reporting across EU member states. The financial crisis, sparked the following year, prompted a substantial tightening of the regulation. Introduced at the beginning of 2018, MiFID II had a seismic impact across the global financial industry. It's been particularly felt in the way operational data is gathered, in how market participants deal with non-EU counterparts and in the way they charge for their services.

Under threat of fines potentially equivalent to 10 per cent of annual revenue, firms spent about $2.5 billion globally in 2017 to make themselves compliant with MiFID II's extensive rules.

One of the regulation's many consequences has been the introduction of surveillance of communications within companies' front-offices, with firms being required to record phone calls and eComms between their employees and clients. As the number and types of communications formats has increased, the regulations have been interpreted also to include social media.

Fast forward another six months, however, and GDPR brought concern and confusion to compliance teams. This sprawling piece of legislation was created to protect the privacy of ordinary people as they generated a tsunami of digitised personal data in everything from online retail purchases and social media interactions to personal banking activities and even household routines.

The GDPR takes a broad-brush society-wide approach to privacy by wresting control of personal data from corporate and government servers and putting it into the hands of individuals. The ePrivacy Regulation, meanwhile, will bring a laser focus on communications, especially eComms and the metadata attached to them. For financial firms, it raises the additional possibility that communications made without involvement of humans – by technology such as the Internet of Things, for instance – will be included in its remit, potentially having an impact on the use of algorithmically executed trading.

On the face of it these dual streams of regulations look contradictory and compliance officers initially fretted that in their efforts to comply with one, they'd breach the other. Since then, a more measured view has emerged.

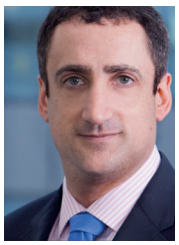
"There was a long period of time where there was just the hands-up-in-the-air panic around the fact that really you have two conflicting regulatory directions of travel," says **Paul Clulow-Phillips**, Managing Director, Co-Global Head of Markets Compliance and Global Head of Capital Markets Surveillance at Société Générale. "A more nuanced view is evidenced now in most organisations."

Private or Public?

Monitoring of front-desk activities is not new but MiFID prompted firms to tighten up on eComms surveillance. Now they have a wide variety of technologies at hand that can capture every word uttered across email, messaging systems, phones and multiple other channels. Initially unsure of just what data they needed to store, firms adopted technologies within a more-is-better policy framework. The threat of a fine that could potentially amount to 10 per cent of turnover was a powerful incentive to gather everything they could.

With the advent of GDPR, however, it became clear this approach could land them with a similarly huge penalty if their surveillance had gathered personal data they couldn't justify storing. Compliance officers' frustrations coalesced around the fundamental requirement that firms differentiate between personal eComms data, which is protected under privacy laws, from that linked to business, which must be kept under MiFID II. For many, it seemed an intractable problem.

"When MiFID II came into force, the concern was around how you force staff to record conversations that might not lead to a transaction in a financial instrument – but my point has always been, you don't know what is private and what isn't", argues **Sam Tyfield**, Partner at Shoosmiths. "Any conversation that anybody has could lead to, or involve, a transaction of a financial instrument. So your obligation is to pretty much record everything."



"Any conversation that anybody has could lead to, or involve, a transaction of a financial instrument. So your obligation is to pretty much record everything."

Sam Tyfield, Shoosmiths

The difficulty in not crossing what **Shiran Weitzman**, CEO of Shield, calls the "thin line between privacy and business" is acutely felt on trading, risk-management and research desks, which have long relied on personal relationships with counterparties and customers. Even in the digital age those personal contacts still matter and when such relationships are more than functional, it's likely business and pleasure will be mixed in conversation.

Mobile Muddle

As firms test the limits of GDPR within a MiFID-compliant environment, an unsurprising focus of their efforts has become mobile phones. While banks and financial firms have been able to keep a lid on things by preventing the use of in-house eComms systems for personal communications, they've found it difficult to maintain control when employees take their conversations off-grid and onto their phones.

Smartphones are more than just communications devices. They store family photos, movies and other digital keepsakes. Surveilling them under privacy laws that strictly limit the amount of personal data a company may monitor has become a sticking point for compliance officers. Firms must have a very good reason to request permission to delve into private data and even then they are shackled by other provisions regarding its storage and future use.

Some firms have dealt with this by issuing their own mobile phones for business use with the explicit agreement that all communications will be monitored and possibly stored. The rationale behind this approach is that should personal information be harvested, then the responsibility for that lies with the user and not the company.

"With that mechanism, you can legitimately say you have given the employee all of the tools that they need to be able to comply with the rules," says Clulow-Phillips. When backed up with policies and procedures, the bank is protected against employees who decide to make non-compliant calls, he added.

"That's their decision. I would see them as being first in the firing line as opposed to the bank in those circumstances."

However, phones are expensive to provide to all compliance-critical staff. A cheaper and more flexible alternative that has gained traction is the granting of permission for staff to use their own mobile phones at work, a policy generally known BYOD – Bring Your Own Device. Generally, they've been fitted with apps enabling employees to separate their private and business communications, or, alternatively they've operated on different SIMs.

But this policy potentially creates even more problems. For a start, many banks have baulked at the very idea of allowing personal phones on the trading floor, creating tension among teams. Credit Agricole has signs around its trading floors explicitly banning their use, said **Anish Kalraiya**, Director of Surveillance and Monitoring at Crédit Agricole CIB.

More importantly, however, there is concern that segregating private eComms from those relating to business can prevent critical information and even signals of criminal behaviour from reaching the desk of compliance officers. Tyfield and Clulow-Phillips are among many who see no alternative to banning all conversation that can't be recorded.

"In an ideal world BYOD wouldn't exist," said Clulow-Phillips. "The minute you introduce personal devices and social media into the equation, that instantly becomes more difficult."

"The minute you introduce personal devices and social media into the equation, that instantly becomes more difficult."

Paul Clulow-Phillips, Societe Generale

BYOD offers other less philosophical complications. For instance, physically taking a phone from someone in order to delete data that may include photographs and movies isn't good for fostering a harmonious working environment, warns Weitzman.

"It might be a challenge for the firm to say, "No, we don't care – we cannot do that, because you signed a paper," he says. "And there will be an argument, and this argument, or this tension, is going to be more and more present in the day to day life of firms."

Multinational firms have the additional headache of managing a patchwork of approaches to privacy protections across their various jurisdictions. The UK's PECR, for instance, takes a less libertarian stand in its application than, say France, where interference in an individual's personal life is severely frowned upon. In other countries, including Germany, unions and workers councils have a greater say in circumscribing an edict's implementation. Whereas in the US, where regulations are seen as more prescriptive, there is far less focus on the privacy agenda, says Clulow-Phillips.

Credit Agricole has offices in Paris and London, requiring the bank to take different approaches in each jurisdiction, explains Kalraiya.

"In the UK, it is permissible for you to go and review, monitor, search, if you want to do a deep dive, dig into something that you might find as suspicious – you don't have any restriction per se in the monitoring that you would undertake for your front office staff, or any staff in general," he says. "That's not the case in France. You can't go looking for something, you do not have the right to go and look at a person's email. They really do take their privacy statements quite seriously."

"In France… you do not have the right to go and look at a person's email. They really do take their privacy statements quite seriously."

Anish Kalraiya, Credit Agricole

Like, Poke or Unfriend?

The identification of compliant and non-compliant material within eComms data is made more difficult each year with the arrival of new social media platforms. By recent estimates some 4.4 billion people use one or more of the almost 1,000 networks on the internet.

While many firms bar the use of Facebook, Twitter and the like on their in-house terminals, the fact that many employees use those networks on their phones has made enforcement tricky. Consequently, access is increasingly being granted under conditions that accounts are vetted first and that content could be scraped under company surveillance programmes.

Firms have backed down partly because so many of their clients use social media, says Weitzman. When a trader needs to stay in touch with a customer who prefers to communicate through LinkedIn or WhatsApp it would be potentially costly to prevent those contacts.

Screen scraping isn't ideal and, unsurprisingly, has met with resistance. It's a blunt instrument to solve a delicate problem and opens firms to potential regulatory sanctions. The GDPR stresses that compliance officers must give specific reasons for collecting data from personal channels such as social media. That means wholesale extraction of eComms data should only be undertaken if it can be proved that doing so is necessary to comply with regulations. It's not sufficient for firms to go fishing to see what they could find; they must have a cast-iron reason, says **Balavernie Sritharan**, a Technical Director at Deloitte.

"Screen scraping data without legitimate interests is not going to cut the mustard," she says. "Firms really need to take a proportionate approach to risk management and understand how they are balancing the organisation's interest against the individual's rights and interest and can they realistically justify the balance. It's quite an important one."

"Firms really need to take a proportionate approach to risk management and understand how they are balancing the organisation's interest against the individual's rights"

Balavernie Sritharan, Deloitte

#EmojiTroubles

To extract pertinent information from the data lakes they amass, compliance officers use sophisticated artificial software applications such as Natural Language Processing and Machine Learning to identify key words, phrases and even speech patterns. Some work better than others – but even the best aren't very good, according to one Head of Markets Surveillance at a large bank, who estimates that the most a firm can expect from their language processors is a 60 per cent accuracy rate, even less when it comes to contextualising verbal communication.

"There's still not a sophisticated way of putting the spoken language into meta-data, and then be able to search through it like you would eComms," he says. "There are always going to be issues with the level of technology in terms of accents and languages, and picking up everything that's spoken."

Adam Clarke, a Director at Deloitte agrees, saying that the evolving nature of language makes it troublesome for technology to weed out problem content.

"The way people use language has now blurred so much and the way people speak to each other so casually at work now, including over email, including over chat and WhatsApp makes it's very, very hard to say that one thing was personal and another was business," he says.

Artificial intelligence tools can be trained to identify many languages, but one they have yet to crack is a form of visual communication that wouldn't immediately spring to most people's minds as a risk to financial firms – emojis. The pictorial representations of emotions in eComms is a growing worry for compliance officers because their meaning is often only understood by their users, making their use difficult to interpret and therefore to justify monitoring. Compliance concern extends to the possibility that they might be deliberately used to obfuscate non-compliant communications.

Criminal Crackdown

MiFID II and GDPR have a regulatory remit to protect investors by, among other things, preventing deceitful practices such as money laundering and insider trading. Observers fear these could be easily circumvented by the use of coded language that compliance software doesn't recognise.

"People are unlikely to say phrases such as, 'Let's spoof the market today', 'let's insider trade'," Clarke says. "People know they're being recorded so it will be more subtle references, single-word or even symbol exchanges, like 'you owe me one' may be represented with a winking emoji."

"People know they're being recorded so it will be more subtle references, single-word or even symbol exchanges, like 'you owe me one' may be represented with a winking emoji."

Adam Clarke, Deloitte

The use of coded language in such a way is not unprecedented. In 2010, the US Securities and Exchange Commission prosecuted UBS Securities investment banker Igor Poteroba for tipping off a friend about potentially lucrative upcoming transactions. In a series of emails in which Poteroba used pre-agreed code phrases to pass on information, he netted about $1 million from illegal trades before 11 merger deals.

That the culprits in the LIBOR rigging scandal openly discussed their illegal plans would only make it more likely that miscreants in the making would redouble their use of coded language, observers say.

The temptation is to put the onus on technology to find a work around. According to Tyfield, however, that's a mistaken strategy.

"We're told that all of these technologies are available, these technologies are developing, these technologies are actually quite useful," he says. "But the view in the market is that many of them don't work in practice."

Clarity and Preparation

Two years into MiFID II and 18 months after GDPR went live, regulators are still keeping a watching brief on their new edicts. The experience, however, has given compliance officers confidence to take on ePrivacy, whenever the EU concludes its revisions to the proposal and enacts it into law. And while they've spent all that time getting their houses in order, many have downgraded their initial doubts about being able to meet the obligations of both.

"The reason people tend to perceive there's a conflict is a lack of understanding between how these regulations work together and why they are here in the first place," says Deloitte's Sritharan. "I'd say that privacy laws are really not there to create burden on business it is just there to make sure that the consumers' or business customers' privacy rights are not compromised."

Failsafes are in place to keep check on firms, she explains. From requirements to inform employees they're being monitored to Data Subject Access Requests, as well as other conditional rights such as the rights to ask for their personal data to be removed from company servers, there are structures enshrined in the regulations to prevent firms deliberately or accidentally over-stretching their surveillance remit.

These can only work properly, observers say, if companies construct considered policies and governance regimes that balance their own interests against those of their employees and customers. Instead of instituting a blanket approach to data gathering, firms should instead codify the scope and limits of the data they need and back that up with robust and enforceable policies.

"The expectation of the regulator is not that you're going to spot every single thing and every piece of non-compliance, but it's that you can demonstrate that you have a sensible process in place, to identify and prevent them from occurring," says Sritharan.

Technology, too, can be better used to identify the information that's really necessary. Improving data quality is making it easier for systems to home in on critical eComms content and software upgrades are at least beginning to grapple with the complexities of extracting meaning from unstructured data, including emojis.

"Let's start by first maintaining a robust and a holistic eComms compliance practice that is combining multiple channels and understanding the correlation between them"

Shiran Weitzman, Shield

But change isn't going to happen overnight, argues Shield's Weitzman. Firms were thrust into the new regulatory environment on the back foot, with infrastructure that was ill-suited to such sophisticated and selective monitoring requirements. To make sure they get it right, compliance officers need to take their time to ensure their existing systems are in sync before seeking out "military grade, or intelligence, technology", he says.

"One of a number of complications in the eComms compliance project is privacy – it's becoming a disruption to the baseline project but banks are not aligned from a strategic point," he says. "Let's start by first maintaining a robust and a holistic eComms compliance practice that is combining multiple channels and understanding the correlation between them… before we are talking about all the sexy stuff"

This article was co-written and sponsored by Shield
www.Shieldfc.com

Financial Markets Insights from The Realization Group, is a series of interviews with thought leaders in financial and capital markets. The purpose of the series is to provide exclusive insights into industry developments, through in-depth conversations with C-level executives and key experts from banks, exchanges, vendors and other firms within the financial markets ecosystem. For more information, please visit **www.financialmarketsinsights.com**

Other topics in the series:

Unlocking the Post-Trade Puzzle: New Approaches to Solving the Issue of Operational Costs in the Post-Trade Environment – Download

Doing the Right Thing: Why financial institutions are banking on accessibility – Download

The crypto challenge: Boosting institutional trading in a fast-evolving market – Download

Singapore's FX Take Off: How Singapore aims to become the price discovery venue for foreign exchange in Asia – Download

Seizing the opportunity; understanding the reality: Capitalising on the growth of instant B2B payments – Download

Accessing Asia Pacific Liquidity: Capitalising on Opportunities in a Rapidly Evolving Landscape – Download

Regulation Technology: Enabling More Than Compliance – Download

Time for a Reality Check: How Close Is the Blockchain Revolution in Capital Markets? – Download

All on the Same Page? Effective Strategies for Successful Innovation in Capital Markets – Download

Capture, Correlate, Analyse: Deriving value from electronic communications data – Download

The Realization Group is a full service marketing and business development services company specialising in the capital markets. Our team contains industry practitioners from both the trading and post trade disciplines and we have expertise equally in the on-exchange and OTC trading environments. We apply our comprehensive set of marketing programs and wide-ranging media and business networks to complement the business development requirements of our client organisations.

www.TheRealizationGroup.com