HERBERT
SMITH
FREEHILLS

March 2017

FCA Future Horizons Conference

Market Abuse - 2022

This paper discusses the potential impact of new technology and learning on tackling market abuse.

The discussion is framed around the following scenario:

> A drone flies low through the trees bordering a test track on which Phaethon plc is conducting the secret trials of a prototype car, the Helios, which it claims will be "the world's most advanced commercially available passenger vehicle" when it goes on sale in three years.
>
> Advance orders for the Helios, in return for a non-refundable deposit, are already being taken.
>
> The drone first films a Helios test run, sending back to its operators images of the car running off the track and crashing into a safety barrier. The drone then lands, un-observed, behind garage buildings alongside the track. The operators use the drone to open up a wireless hotspot which mimics that of Phaethon and several Phaethon engineers mistakenly use it, allowing the drone operators to infiltrate Phaethon's network.
>
> The operators of the drone, a group closely linked to the government of Hyperborea, now have access to information confidential to Phaethon, including details of Helios' on-board computer systems as these are developed over time and prior information about company announcements.
>
> Phaethon shares are listed. The share price falls when, several days after the event, the company makes an announcement about the crash filmed by the drone. However, over the next 30 months, the company's share price rises 250% in anticipation of launch date and off the back of announcements about positive test results and strong advance orders.
>
> The drone operators first make a handsome profit on a short position, quickly built up after viewing images of the crash. Thereafter, they commence routinely to trade ahead of Phaethon company announcements. They trade using a group of minor officials working in Hyperborean embassies around the world and through various complicit traders.
>
> Meanwhile, one of the drone operators decides to make some private profit by using the dark web to sell price-sensitive information about the Helios.
>
> As launch date approaches, the drone operators sell their remaining stock, use their trading network to establish a short position and then launch a serious of cyber-attacks which disrupt the Helios' on-board computer systems leading to a fatal accident and a huge fall in the Phaethon share price.

None of this should strike the reader as fanciful.

The FBI's List of Most Wanted Cyber Criminals currently includes several suspects who are alleged to have links to foreign governments[1]. The resources at their disposal may be very substantial.

The use of drone technology for industrial espionage has already led to the establishment of an industry to counter such activity[2].

Cyber-attacks, including infiltration and disruption have become all too familiar[3].

Several cases of computer hacking have, allegedly, been motivated by a desire to secure pre-market access to price sensitive information. For example, the infiltration of an information vendor[4].

[1] https://www.fbi.gov/wanted/cyber

[2] The scenario would be in breach of Civil Aviation Authority regs that prohibit flights close to structures! https://www.caa.co.uk/Consumers/Model-aircraft-and-drones/The-Dronecode/

[3] In general, this paper does not discuss the remedies available to Phaethon against the drone operators. See, in particular Directive on Attacks Against Information Systems, Directive 2013/40/EU and, in the UK, the Computer Misuse Act 1990

What is public information?

Was the information about the car crash at the first test, publicly available?

The UK regulators have discussed the issue in the Market Abuse Chapter of the Handbook (MAR) using the by now well-known example of a passenger on a train who passes a burning factory, calls their broker and sells shares in the factory owner. The train passenger is said to have obtained information about the factory owner, legitimately, by observing a public event (the fire)[5].

Associated commentary in MAR, refers to information that can be obtained by members of the public without infringing obligations of privacy, property or confidentiality[6].

Assume, in our scenario, the drone hovers just outside the perimeter fence of the test track as the crash is observed, what obligations are infringed?

Is this corporate espionage or simply the clever use of technology to secure a legitimate advantage?

The location of the fence should not be the determining factor: the train passenger in the FCA's hypothetical presumably looks through or over a fence. In other circumstances, a person standing outside a depot counting the trucks as they enter and leave might discern valuable information about a commodity stored there. Would or should it be any different if that information was gathered using a drone hovering above the site or a satellite in orbit?

The chance nature of the observation from the train also seems an insufficient basis for distinguishing the two cases.

The potential exists, therefore, for significant information asymmetries even if only of that duration that may be exploited by those who have the means to do so. In our scenario the company's announcement to the market is not timely but a delay of only an hour would have been ample time to exploit the position. Conceptually there is nothing new here but practically we should expect the issue to become more common.

UK regulators have also discussed public availability of information in the context of the Internet. The general conclusion has been that information is regarded as generally available, if available through the internet or some other publication, even if only available upon payment of a fee[7].

Is the information being sold on the dark web publically available?

There seems no reason in principle to distinguish the dark web from the Internet. Sites on the dark web cannot be identified using traditional search engines but the software is available to access sites with an ".onion" domain name and the need to pay a fee is not conclusive on the FCA's analysis[8].

MAR prohibits the use of a "tip" where the recipient knows or ought to know that the tip is based on inside information. Here there is a good argument that sale of the information on the dark web suggest it has been obtained without consent.

The "infringement of rights of privacy, property or confidentiality" would presumably be sufficient to ensure the information was properly to be regarded as "non-public".

Of course, all that assumes anyone concerned with the integrity of the market knows that the information is being traded on the dark web. No financial institution would, today, be expected to encompass the dark web within its routine surveillance of trading but is there a case for some level of surveillance, for example by an assurer in respect of information about itself? The regulators may, need to take a more systematic approach to monitoring of the dark web: apparently a place for boasting of cyber-attacks but also of recruiting ground for attackers. [9]

[4] https://www.justice.gov/usao-nj/pr/ukrainian-hacker-admits-role-largest-known-computer-hacking-and-securities-fraud-scheme
[5] MAR 1.2.14
[6] MAR 1.2.12
[7] MAR 1.2.12(3)
[8] https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/
[9] www.bbc.co.uk/news/technology-37974776

How might surveillance for this kind of behaviour change in the years ahead.

First, I would expect the information demands made by regulators to significantly increase.

To date, the most significant changes in data demands have been in respect of prudential information. The demands made of banks in the US to provide information under the Comprehensive Capital Analysis of Review (CCAR) being the most prominent example. There are signs that attention is now turning to information that may assist in detecting trading misconduct.

The SEC has announced the establishment of the Consolidated Audit Trail so that regulators will have more timely access to a comprehensive set of trading data, in the expectation it will enable it to more efficiently and effectively conduct research, reconstruct market events, monitor market behaviour, and identify and investigate misconduct[10].

Following an October 2016 meeting with industry convened by the US Treasury, Federal Reserve Board, SEC an CFTC, the regulators emphasised a continued focus on data in respect of the market in US Treasuries.

But that is likely to be only the beginning – a foundation on which to build other surveillance and monitoring programmes. MiFiD II, when it comes into force will, of course, subsequently increase the volume of available information.

Other regulators and exchange operators have announced that they are working with software developers to use computing power to enhance their monitoring and surveillance programs through the use of artificial intelligence[11]. For example, ICY, pronounced “I see why”, is the new monitoring system that the French AMF is developing internally with the backing of an external software company. It will be based on Big Data technologies that will allow the AMF to quickly screen data representing large and varied trading volumes. Starting in the second half of 2017, ICY will gradually be rolled out to start receiving MiFID II data from 3 January 2018.

The objective must be to bring together trading data and other information, including communications data in an effort to identify potentially abusive trading. Regulatory demands for the requisite level of additional information may raise privacy concerns (at least in Europe) and substantially increased demands on firms to provide data in a form that could be used by a regulator may be costly. I would expect discussions amongst regulators to explore whether there is a common view about what is reasonable and proportionate.

Inevitably, regulators will expect more of individual firm surveillance. Several firms have, of course, already begun to consider how different data sets might be looked at in a consolidated way to identify potential areas of concern or, at least, identify matters justifying further enquiry. These efforts have generally been quite modest; aggregating trading data; surveillance of written communication; revenue numbers; hours spent in the office; incidents of cancelled or corrected trades trader might in various combinations suggest the need for follow-up. Poor quality data and a concern about high levels of "noise" or false positives and the challenge of identifying what normal looks like have so far constrained these efforts and led to scepticism about preferred "big data" solutions but better managed data, smarter software and greater computing power will mean scepticism gives way to far more sophisticated matching of data.

The limitations of lexicon based communication surveillance were apparent in the various rate-setting and FX-trading enforcement cases of recent years. The traders involved scarcely used recognisable words in many cases and communications that came to be seen as problematic did not stand out using lexicon based searches. The use of machine learning (predictive coding) an approach now being used in large document retrieval exercises, will surely have potential application in a surveillance context. Identifying patterns of communication that could form the basis of alerts should be possible as a supplement to lexicon based searches and will surely become an input into a search for "abnormal" behaviour.

[10] https://www.sec.gov/news/pressrelease/2016-240.html

[11] See, for example: http://uk.reuters.com/article/us-exchanges-surveillance-ai-idUKKCN12P0FJ?il=0 ; http://www.digitalreasoning.com/buzz/nasdaq-and-digital-reasoning-establish- exclusive-alliance-to-deliver-holistic-next-generation-surveillance-and-monitoring-technology.1884035; http://www.amf-france.org/en_US/Actualites/Communiques-de-presse/AMF/annee-2017.html?docId=workspace%3A%2F%2FSpacesStore%2F0fc52391-54c8-44bf-a134-bd6f7ebd1430

Voice surveillance remains a much neglected area. Again short-comings in the currently available software explain the limited progress to date. Much of the software is, at present, characterised by poor accuracy in recognising words. It is, however, possible to improve the accuracy of the out-of-the-box software: that generally needs to be done desk by desk and firms will face some of the same challenge as lexicon-based searches of written communication – in a surveillance context you will not always know the words which indicate a problem. The technology is improving but, for example, a multi-language communication is likely to confuse a system notwithstanding that it has the capacity to monitor in many languages. Recognition of basic emotions seems some way off but will surely become available.

Regulators have generally stopped short of setting expectations for voice surveillance but that will change as the software improves and processing power increases, for example, through use of the cloud.

In UK regulatory terms, the reasonable steps necessary for a Senior Manager to show that the business of the firm for which they are responsible is controlled effectively, are changing. That is particularly so given the requirement to record telephone lines used for the receipt, execution or arranging of client orders[12]. Nonetheless, in our scenario, the traders will surely seek to cover their tracks by using "privately owned equipment" even though a firm must take reasonable steps to prevent that[13]. By today's standards it would be a very effective Compliance Department that spotted the absence of an instruction on a recorded line or an electronic communication that corresponded to an order actually placed but that too may change with improved data, better software and increased computing power.

Routine trade surveillance typically operates by highlighting departures from expected patterns of trading: as noted, many banks have embarked upon enhanced surveillance predicated on assumptions about expected patterns of behaviour.

The expected behaviour may be as simple as typical hours spent in the office, the taking of annual leave or the number of cancelled and corrected trades. But it could be far more subtle. The use of medical science in trader surveillance is one area that is likely to develop significantly in the next 5 years.

A group of Cambridge researchers recently simulated a trading floor in the lab by having volunteers buy and sell assets amongst themselves. They measured the volunteers' natural hormone levels in one experiment and artificially raised them in another.

When given doses of particular hormones, the volunteers invested more in risky assets. The researchers' conclusion: "Our view is that hormonal changes can help us understand traders' behaviour, particularly during periods of financial instability,"[14] Subjecting traders to a blood test when they arrive for work each morning may seem far-fetched but the drug-sniffer dogs that patrol the lobbies of some Hong Kong office buildings with bank tenants might also have seemed far-fetched just a few years ago.

A second group of researchers looked at interoception the sensing of physiological signals originating inside the body, such as hunger, pain and heart rate. People with greater sensitivity to interoceptive signals, as measured by, for example, tests of heart beat detection, perform better in laboratory studies of risky decision-making. The researchers found that traders are better able to perceive their own heartbeats than matched controls from the non-trading population. Moreover, the interoceptive ability of traders predicted their relative profitability, and strikingly, how long they survived in the financial markets![15]

And this is surely just the beginning?

In our scenario, it might have been possible to detect the abusive trades through the straightforward monitoring of trading ahead of an announcement but, experience shows, such trading generally goes undetected, at least until greed encourages the wrong-doer to overplay his hand.

[12] FCA Handbook COBS 11.8.

[13] See COBS 11.8.5A.

[14] http://www.cam.ac.uk/research/news/traders-hormones-may-destabilise-financial-markets#sthash.Uw0ZNAW0.dpuf

[15] http://www.nature.com/articles/srep32986

What if the employers of our complicit traders had fitted the traders with monitors tracking changes in heart rate and other vital signs? An MIT study fitted traders with wristwatch sensors measuring pulse and perspiration with the potential to identify, in real time, a trader undergoing unusual levels of stress[16].

There may be an initial response that such intrusive surveillance is a step too far. "Orwellian" and unacceptable but conceptually it might be thought of as merely an extension of existing surveillance: the routine surveillance of email, even though they are known to contain private data (albeit a breach of bank use policies); the monitoring of entry and exit from the workplace; those drug sniffer dogs in Hong Kong. It would be relatively simple today to track a trader's whereabouts by asking him or her to wear a tracking device, or by simply inserting a chip into their access card. Banks invest considerable time and money on physical information barriers to limit the risk of unauthorised access to non-public price sensitive information but perimeter defences are easily breaches by "tail-gaters" accessing areas without permission. How strong is the ethical objection to an alert that signals to Compliance, in real time, that a public side employee has crossed into a private side area?

In 2022, science and technology will have radically changed the way in which regulators and firms seek to defect and prevent market abuse. It will need to, because those who wish to commit market abuse will use that same technology in increasingly innovative ways.

Herbert Smith Freehills LLP

[16] http://www.bloomberg.com/news/articles/2016-09-01/wall-street-s-next-frontier-is-hacking-into-emotions-of-traders