Using Social Media as a Source of Financial Intelligence: A New Frontier in the Fight Against Crime?

Florence Keen

Financial institutions are an indispensable ingredient in the fight against money laundering and terrorism financing. Recently, some of the major ones have been showing interest in the vast amount of personal information available within social media and its potential role in the investigation of suspicious activities. Could social media sites become the go-to platforms for financial service providers as they assess their clients? What are the implications of using open-source tools for security and crime-fighting purposes?

The amount of data is expanding at an exponential rate. It is estimated that the amount of data collected on digital platforms each day is equivalent to eight times the information stored in all of the libraries in the US. Unsurprisingly, the source of the majority of this data is the ever-increasing content – including personal information – that is uploaded onto social media networks.

The proliferation of social media over the past decade has profoundly altered the way human beings interact, from the way they form relationships to the portrayal of themselves in public spaces and, now, to the many ways in which individuals can be identified, profiled and assessed by private and public entities alike. The range of available platforms is seemingly infinite, with the most prominent being Twitter, YouTube, Instagram and, of course, Facebook, which has recently reported holding over a billion active users.

Recruitment agencies, among others, are known to scan social networks when evaluating potential employees and, increasingly, services require customers to have a social media profile in order to access their products. An inescapable fact of modern life is that participating fully in society means accepting – and allowing, through terms and conditions outlined in the small print – that much of what you do will have a digital and social media footprint and unintended end-user consequences.

The harvesting of both open and closed sources of social media is a prominent weapon in the fight against criminality, including financial crime.

The new flood of information presents immense opportunities for a range of different stakeholders from the commercial as well as the security sectors. Data retrieved from social media are a commodity in itself, through the ability to offer quantifiable insights into human behaviour and customer preferences, a fact evidenced by the success of data mining and analytics.

The potential of social media intelligence (hereafter SOCMINT – a term first coined by researchers for the Demos think tank in 2011) has not gone unnoticed by law enforcement and the security services; the harvesting of both open and closed sources of social media has become a new surveillance technique and is a prominent weapon in the fight against criminality, including financial crime.

As criminals move their operations online, the use of information passing through social media platforms has become essential for the development of appropriate business knowledge. Information derived from social media has been used to expand law enforcement agencies’ knowledge of criminal networks and their communication patterns, of extremist views and terrorist ideologies, as well as the planning or expression of anti-social behaviour. SOCMINT has the potential to become a productive instrument in the battle against financial crime for a wide range of interest groups, from law enforcement to global financial institutions to FinTech start-ups offering bespoke financial services.

However, the use of SOCMINT as financial intelligence (FININT) highlights the fact that, unlike law enforcement agencies (which have the authority to investigate private information if deemed ‘necessary and proportionate’), the private sector can only seek out information that is publicly available, on ‘open’ social media profiles. Yet the practice of collecting SOCMINT as FININT is
ethically and legally more complex than the more traditional intelligence-gathering techniques carried out by law enforcement.

Firstly, the private sector is neither recognised nor accepted as an ‘overseer of security’. Secondly, the use of personal information for financial intelligence by the private sector may entail the collection and processing of information for purposes for which consent was not given. Finally, its usefulness is limited by individual user privacy settings, which could potentially lead to misinformation.

Nevertheless, international and domestic legislation to tackle anti-money laundering and terrorism financing – including the UK’s Money Laundering Regulations of 2007 and the EU anti-money laundering (AML) directives – now places significant pressure on the private sector to pursue new methods of investigation, including the extraction of data from social media sources.

In 2013, the Financial Action Task Force (FATF) – the body responsible for setting global standards against money laundering, terrorist financing and proliferation finance – identified social media as a means to verify the accuracy of customers’ personal declarations about their sources of wealth, one that could reveal crucial information about a person’s lifestyle and income sources. The use of this tool as a legitimate source of information has since gained further attention from businesses subject to FATF standards as they attempt to implement the FATF’s requirements.

Given the increasing levels of responsibility that financial institutions in the private sector are being expected to assume (in particular acting as the first line of defence against money laundering and terrorist financing), the increased use of SOCMINT in the advancement of financial intelligence is not only logical but predictable. A few leading major financial institutions are currently considering drawing on social media sources when conducting enhanced customer due diligence checks in cases where these are required by the institution’s regulator or internal policies.

However, information gathered through social media has so far been useful primarily as a supplement to other – more conventional and official – forms of identity assessment, such as national ID cards or other state-issued documents. The reliability of this information is, of course, open to debate. Is information on social media truly a reflection of an individual’s character? Is the absence of a social media presence evidence of suspicious activity? Before its use as FININT can be properly sanctioned, policymakers must decide to what extent information about someone gleaned from social media should be used to influence decisions, particularly on something as important as the provision or termination of financial services or, on a more advanced level, the initiation of criminal investigations.

Leading financial services providers are keen to determine whether social media is as promising a source of intelligence as organisations such as the FATF have suggested. Some of the most commonly identified obstacles to its use as a reliable intelligence-gathering instrument relate to the lack of detail that characterises the information, as well as the inability to distinguish between individuals with common names, nicknames or multiple accounts. Other analytical difficulties arise from the fact that individuals may communicate in different languages or in slang, thus complicating the investigators’ assessment and network-building capacity. Furthermore, by its very nature, social media is ephemeral, with content created and deleted regularly, often after short periods.

The prospects for mainstreaming the use of social media as a source of FININT and due diligence will also depend on overcoming the various ethical debates that surround it. Is it appropriate for private entities to use personal information – despite it being available in an open source – to complete assessments on individuals? In practice, the use of these tools by law enforcement agencies is limited to occasions where there are initial grounds for suspicion. Should the same apply to their use by the private sector?

In addition, as the commercial value of social media data increases, its ‘mining’ by private entities will almost inevitably put certain clients at a disadvantage. Social media privacy settings can be expected to become increasingly more complex and difficult to navigate as social media platforms respond to commercial attempts to access open source data.
The use of SOCMINT for the purposes of FININT in practice involves the large-scale monitoring and collection of personal and behavioural data of clients regardless of status, background or political affiliation. Civil liberty concerns over the prospect of an Orwellian ‘surveillance state’ and the tensions between the interests of individual privacy and national security once again become issues of public interest.

While it is true that financial institutions currently only have access to open source data, objections to big firms monitoring individual activity are perfectly reasonable. There is no clear guidance on the complex legal and ethical issues surrounding this emerging practice and its impact on the individuals involved.

Looking to the future, private entities using social media data will also need to consider the prospect of civil liability in cases where consent ‘for processing personal data’ in specific circumstances might be questioned in court by more dedicated privacy defenders.

The use of SOCMINT as a tool for the private sector to expand its FININT is still in its infancy, and many questions need to be addressed. Does data collected through social media merely lead to the generation of additional ‘red flags’ for financial institutions, rather than actually contributing to the simplification of the monitoring of suspicious behaviour? Has there been an impact assessment of the pros and cons of adopting this approach?

Information gleaned from social media may yet prove invaluable as FININT, but not unless analysts and policymakers have a clear understanding of its advantages and disadvantages, the correct legal framework for its use, and an appreciation of the ethical issues that accompany its use as FININT.

While SOCMINT and its many applications may seem attractive, it is clear that little assessment has been made of how precisely this source of information can be exploited. Any such assessment needs to consider the difficulty of distinguishing fiction from reality on social media, as well as appreciating the civil liberties issues involved, such as the proportionality of the level of intrusion in relation to potential gains, as well as the utility of pursuing this route in preference to other, less controversial, investigative practices.

Florence Keen
Research Analyst, Centre for Financial Crime and Security Studies, RUSI.

Beijing’s North Korea Policy in 2016: Keep Calm and Carry On

Adam Cathcart

Although North Korea’s nuclear and missile tests have rocked the relationship with China, both sides seem intent on keeping calm.

Applying metaphors to Beijing’s relationship with North Korea is a difficult business. In recent years, China’s old bonds of brotherhood with North Korea have given way to a wary and often openly sceptical mutual outlook. The Chinese Communist Party’s (CCP) preferred metaphors for the relationship now rest on ‘shared mountains and rivers’, an ideologically neutral reference to the shared 1,400-km riverine boundary, but just as often, Chinese editorials note that the relationship is ‘in the ditch’ or that ‘North Korea is walking on a tightrope’ with Beijing. For its part, North Korea has refused to play a role in one particularly potent metaphor – Chinese President Xi Jinping’s frontier trade- and influence-expanding One Belt, One Road policy – and has turned its back on Beijing on multiple occasions while brandishing the ‘treasured sword’ of its nuclear capability.

North Korea’s fourth nuclear test on 6 January 2016 had been telegraphed three weeks prior by Supreme Leader Kim Jong-un himself. In remarks made from a 1940s-era small-arms factory and firing range, he alleged that North Korea would soon demonstrate hydrogen bomb capabilities to the world. While Kim’s play-acting in what amounts to his grandfather’s clothing is now de rigueur, the timing of his statement was anything but: a large Korean People’s