GIR
Global Investigations Review
NEWS

Too big to care? What should Big Tech learn from banking?

13 May 2019

Simon Taylor and Rob Mason

Tech companies need to implement effective compliance programmes to avoid increasing regulatory scrutiny and fines that could far exceed those imposed on banks following the financial crisis, Forensic Risk Alliance partner Rob Mason and director Simon Taylor argue.

Twenty-five years ago Facebook, Google, Amazon and other tech giants did not exist. In the years that followed, a generation of tech entrepreneurs jumped into to the vacuum of regulation left by governments and created the most valuable corporations in the world using personal data collected from individuals to generate profit.

Having now woken up, politicians and regulators are faced with a number of problems including: how to reign in the power of these organisations; how to restore healthy competition; how to ensure that personal data entrusted to Big Tech is used responsibly and in accordance with the terms on which it was provided; how to prevent the spread of harmful content through their platforms; and how to regulate political campaigning on their platforms.

These problems are generating a "techlash"' by governments around the world, with proposals for breaking up the Big Tech monopolies mixing with calls for tough regulation. The US, having arguably been left behind by the EU with its passing of the General Data Protection Regulation (GDPR), will not be for long. Proposals for tech regulation will be an important issue in the 2020

First published on the *Global Investigations Review* website, May 2018

US Presidential election and will be high on the agenda of the next, if not the current US President.

Against this stand the tech giants themselves, and in particular Facebook, while ready to accept that the scale of the problems cannot be handled by self-regulation alone, are keen to have a hand in shaping any new rules.

FTC v Facebook

Unlike banking and other corporate actors, Big Tech is yet to experience the full scale of what regulatory action might look like. However, the ongoing US Federal Trade Commission (FTC) case against Facebook (in respect of which Facebook recently set aside $3 billion to cover a potential fine which may well rise to $5 billion) is likely to be the first among many.

In 2011, the FTC launched investigations into Facebook's privacy practices. The FTC issued an eight-count complaint against Facebook for various breaches involving the sharing of private consumer data to third parties. The FTC and Facebook entered into a consent decree order on 10 August 2012, which prevented the tech company from making any further deceptive privacy claims and to receive "affirmative express consent" before changing the privacy or security of consumer's personal information. It also imposed biennial independent third-party audits on Facebook for the next 20 years (PwC last reported on 12 April 2017 and a further report will be published soon).

Although numerous complaints have been made against Facebook in the intervening period, the FTC has not, until recently, suggested that Facebook be charged with violating the consent order. Significant complaints since the order include, but are not limited to:

- Senator Ted Cruz's Presidential campaign in 2015 – a small data company, indirectly financed by Ted Cruz's billionaire benefactor reportedly paid researchers at Cambridge University to illegally gather psychological profiles of US electorates using US Facebook users private information;
- Patient Privacy Breaches – using its "Groups" product, Facebook was accused of deceptively sharing the personal health information of its consumers, including groups for Alcoholics Anonymous, Gender and sexuality groups including groups for Transgender children and various forms of cancer sufferers' groups; and
- Software bugs – Facebook admitted that software bugs created privacy concerns for up to 14 million of its users as privacy settings were unknowingly changed and another software bug "unblocked" people that hundreds and thousands of users had previously blocked, creating a safety and risk issue for affected users.

The FTC opened fresh investigations against Facebook in March 2018 following revelations by a former employee of UK consultancy Cambridge Analytica. The data collection was allegedly facilitated by Aleksandr Kogan, a data scientist, using a questionnaire that took advantage of a loophole in Facebook's API allowing data to be collected from users who took the quiz as well as their "friends". Kogan denies the allegations.

How big could fines get?

One of the key open questions will be how much a data misuse might cost. The FTC has the power to impose a penalty of up to $41,484 for each violation of the Federal Trade Commission Act. Disclosure of a single individual's personal data to a single third-party without consent may be considered a violation. In April 2018, Facebook disclosed that personal information of up to 87 million people, including over 70 million Americans, may have been improperly shared with Cambridge Analytica. In theory, this provides the potential for the FTC to apply a penalty of several trillion dollars, an amount that would threaten the viability of Facebook as a going concern. However, the $3 billion legal expense accrued by Facebook against the ongoing FTC inquiry is a small fraction of this, which still left Facebook reporting well over $2 billion of net income for the first quarter of 2019, after the legal expense had been deducted.
Data breaches tend to be systemic in nature. Facebook has well over 2 billion monthly active users worldwide of which over 240 million are in the US and Canada. In contrast, the maximum penalty which the FTC could levy for a mere 25,000 violations is over $1 billion.

In Europe, the fines for "especially severe" violations of the GDPR are up to 4% of global turnover. Alphabet, Google's parent company, which had worldwide revenues of over $136 billion in 2018, was fined €1.5 billion ($1.7 billion) by the European Commission in the first quarter of 2019, yet still reported quarterly net earnings of $6.7 billion, almost four times this amount.
With the FTC apparently unwilling and the European Commission unable to leverage penalties greater than amounts which, in the view of many commentators, are regarded simply as a cost of doing business, how will regulators act to bring these tech giants into line?

Deeper, tougher regulations?
Fines of the scale anticipated are unlikely, on their own, to bring about the cultural changes required by governments. Given the importance and value of the tech sector commercially and socially (the top four tech companies – Google, Apple, Amazon, Facebook – have combined market capitalisations of $3.3 trillion, more than twice that of the top four banks) together with the enormous commercial value of the personal data deposited with tech companies, it is likely that governments will look to areas such as banking for inspiration.

Personal liability for executives involved in corporate misuse of data for profit will be high on the list of priorities. Both criminal liability and regulatory enforcement are predictable responses. Mark Zuckerberg's testimony to the US Senate and House committees was littered with promises that his team would "follow up" or "get back to" them, leaving it unclear who knows the answers to important questions. In the UK, the senior managers' regime was imposed on the banks following the financial crisis to avoid executives slipping through the net by shifting responsibility onto others. Perhaps something similar could be applied to tech companies, requiring named senior executives to take personal responsibility for specific aspects of regulatory compliance.
That leads on to the question of regulation more widely and whether the current registration and light-touch supervision system for all entities handling personal data is really fit for the purpose of regulating Big Tech companies whose raison d'être is to collect, analyse and use personal data for profit. For these so-called 'tech platform' companies, who are in the data business and who open their platforms to third-party developers, the need for a different type

of regulation is compelling, one which requires, like banking, licences and authorisations before being permitted to operate. This could also include a "fit and proper person" requirement for senior executives. Although lawmakers, particularly those in the US, do not want to see Big Tech regulated "to death", it is clear that significant changes are required – and will be coming.

More regulation … more compliance

Ten years after the financial crisis, Citibank reported that 15% of its workforce (30,000) worked in compliance, risk and other control functions, while in 2008 it was just 4%. Big Tech may have started on the path of developing compliance programmes (see for example Facebook's new general counsel, a cross-border regulatory enforcement lawyer) but it needs to go further faster.

Comprehensive risk assessments are essential prerequisites of any compliance programme, but identifying and assessing the likelihood and impact of risks could be particularly challenging for tech companies.

The nature of tech companies and their businesses will produce risk assessment and compliance challenges that have not previously been seen in "analogue" industries. "Third parties" are one of the top risks for many companies and typically include agents, country sponsors, lobbyists, suppliers, distributors, partnerships and joint ventures. As well as these "classic" third parties, which are well understood, tech companies also place extensive reliance on large numbers of third-party developers, who not only differ widely in terms of size and complexity, but may also be transitory in nature. These third-party participants are essential for innovation and creativity, but on-boarding them, conducting due diligence and monitoring their behaviour will be fraught with new compliance problems.

Another area, unique to tech companies, is the risks relating to the integration of artificial intelligence and machine learning into platforms and related data sets. By design, the actions and activities of these technologies are difficult for humans to predict and the connections made between, and the uses for, apparently disparate data sets may produce entirely new risks.

Underpinning all of these complexities is the basis for tech companies holding and processing data itself i.e. "informed consent". During the Facebook Senate and House hearings, Senator John Kennedy reportedly said Facebook's user agreement "sucked" and Mark Zuckerberg acknowledged that most users probably didn't read all of it. Consent is, as governments are now alive to, a situation-specific concept. Providing terms and conditions governing the potential use of personal data that are so broad as to become meaningless is no longer acceptable. The implications of this for risk management are significant. Tech businesses change far more rapidly than other industries and the agents of change can be third-party developers and artificial intelligence. The lawful basis for the continued use of the data must keep pace with these changes.

First published on the *Global Investigations Review* website, May 2018

Conclusions

Big Tech needs to brace itself and be prepared for a big change. Tough regulation has been avoided for a long time but it is surely now on its way. Banks initially reacted slowly to the changing regulations and increased compliance and risk staff incrementally. Banks have paid the penalty for that delay – in the region of $345 billion since the financial crisis. To avoid fines that could be even bigger than in banking, and to avoid executives seeing jail time, tech companies need to scale up quickly, understand the risks they face and implement effective compliance programmes.

First published on the *Global Investigations Review* website, May 2018