Cybersecurity, Data Privacy & Information Management Alert

Weil

March, 2020

Big Data Analytics and AI – the need for data governance

By Barry Fishley and George Mole

Barry Fishley
View Bio
barry.fishley@weil.com
+44 20 7903 1410

George Mole
View Bio
george.mole@weil.com
+44 20 7903 1367

Today, data is a valuable asset for *all* organisations, not just 'tech' companies. Regardless of sector or geography, organisations are using an exponentially increasing amount of data from a variety of sources. These large datasets, if exploited correctly, can bring organisations new and exciting business opportunities from 'big data' analytics. If mishandled, however, they may expose organisations to serious legal, reputational and financial consequences; the impact of which will only be magnified for organisations seeking to rapidly develop (or incorporate) innovative tech solutions into consumer-facing products, for example Insurtech and Fintech.

So how can organisations use big data analytics to exploit data without falling foul of privacy laws and what should investors consider when seeking to understand the risk profile of a target.

What is big data analytics?

Big data analytics refers to the analysis of extremely large data sets, often collated from a variety of sources, which are difficult to analyse using traditional data analysis methods. Historically, organisations found it difficult to develop valuable insights which could inform decision-making from big data in a cost-effective and efficient manner. Now, artificial intelligence ("**AI**"), in particular machine learning technology, is acting as a tool for organisations to "unlock" the value of big data due to its ability to analyse various shapes, sizes and forms of data with great speed and accuracy.

Data analytics vs. data privacy

Using big data analytics methods can, however, sit juxtaposed with a number of the underlying principles of the General Data Protection Regulation ("**GDPR**") and other privacy laws. These conflicts can arise in a number of scenarios:

- ***Opacity vs. transparency:*** Using AI to analyse big data makes it difficult to understand the rationale behind the decisions that are being reached as a result of that analysis. This conflicts with the principle of transparency which, under the GDPR, requires that data subjects are presented with certain information about how their personal data is being processed in a "*concise, easily accessible and easy to understand*" manner, using "*clear and plain language*".
- ***Maximisation vs. minimisation:*** Data analysts want to collect as much data as possible to speed up the development and market impact of their tools and products – this is understandable considering the vast

amounts of data available from a plethora of sources; social media, web cookies, IoT devices and wearables to name just a few. This can conflict with the principle of data minimisation, which requires that only personal data which is necessary for the purpose for which it was collected should be processed.

- ***Expansion vs. limitation:*** Similarly, it's not unusual for data analysts experimenting with large datasets to want to repurpose (or expand) the scope of use of that data. This can conflict with the principles of transparency and purpose limitation. For example, mobile phone data can technically be used to analyse footfall in a retail centre but, unless it was collected for that purpose, it shouldn't be.
- ***Automation vs. objection:*** AI relies heavily on automated processing to sift through large datasets with speed and accuracy. This can conflict with the right of data subjects to not be subject to solely automated decisions, including profiling, which have a legal or similarly significant effect on them (although certain exceptions apply). Automated decisions are those made solely by automated means without human involvement. For example, "Smart" lenders in the Fintech sector, rely on automated decisions to speed up what would traditionally be termed 'back' and 'middle' office operations, so as to reduce headcount. This is undertaken by collecting and processing personal data from a wide range of sources using AI to automatically decide whether or not to grant a loan application, and if so the interest rate. This kind of processing poses an additional reputational and legal risk to organisations. Consider the impact on the lender if it was reported that the AI had (intentionally or otherwise) resulted in the business charging higher interest rates to people within a certain demographic.

Tougher consequences for regulatory non-compliance

The consequences of non-compliance with privacy laws can be severe and only seem to be getting tougher. Organisations can attract adverse publicity, suffer damage to their brand and reputation, and in addition be publicly censured by privacy regulators.

Organisations which infringe the rights of data subjects may be subject to administrative fines of up to €20 million or, in some cases, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Recent enforcement action by privacy regulators has shown that these statutory provisions are not idle threats nor just reserved for 'tech-heavy' businesses. In July 2019, the UK Information Commissioner's Office announced its intention to fine British Airways £183.39 million and Marriott International £99.2 million for infringements of the GDPR resulting from their respective data breaches.

In addition to sky-high fines, an increasing number of class action claims are being brought across Europe for breaches of privacy laws. In October 2019 the Court of Appeal, in its judgment in *Lloyd v Google*, allowed a US-style (opt-out) representative data protection class actions to proceed in the UK. This paved the way for the class action claims facing British Airways (from customers affected by the airline's 2018 data breach) and the supermarket Morrisons (from staff who had their information leaked online in 2014).

So, what's the solution? It's data governance

To mitigate these risks, some organisations (but not all) have decided to invest in developing effective data governance frameworks which consider privacy at all stages of the data processing lifecycle. Such frameworks should give the board oversight over the organisation's processing activities and allow it to identify particular risks and/or opportunities to act on.

As a first step, organisations should appoint a committee which has oversight over all processing activities – a privacy or data committee. This committee should be comprised of stakeholders from across the organisation including the data protection officer, general counsel and/or head of compliance. In turn there should be some direct or indirect reporting to the board.

Teams wishing to carry out a new processing activity should carry out a data protection impact assessment ("**DPIA**") and submit that assessment to the committee for approval. DPIAs are required to be carried out for certain processing activities

(which can include data analytics including automated decision making and profiling). However, carrying out DPIAs before conducting *any* new type of data processing is a useful way for organisations to assess the risks associated with the proposed processing, identify which measures they should introduce to mitigate those risks and demonstrate the adoption of a privacy-by-design approach which complies with the GDPR. Processing should not be undertaken until the committee has given its approval and any conditions to that approval have been fulfilled.

Example (Insurtech): How privacy-by-design works.

Consider an insurance company wishing to develop a new mobile app for its customers to view their policy and account details and submit information relating to claims. If a DPIA is carried out during the software design phase, the software developer will be able to implement specific features that comply with the data protection principles. This could include ensuring that the user-interface brings up notifications about the existence and the purpose of the automated decision-making process, provides the user with a dedicated page to oppose an automated decision and express their point of view. In the background, special categories of data (such as health information) entered in certain data fields could be anonymised or pseudonymised in the company's IT system and all data could be mapped on collection in such a way as to improve the ease and efficiency of responding to data subject requests, implementing the organisation's data retention policy and facilitating third party audits.

Once the processing activity has been approved by the committee, data mapping systems and appropriate access controls should be put in place to help identify and manage data once it has been collected. This will help the organisation simplify the process for responding to data subject requests, identify ageing data to help enforce its data retention policy and ensure that it has a record of where, how and whom data is processed by or shared with – which should be on a "need-to-know" basis.

Organisations which engage in automated processing should also ensure that their privacy policies and customer contracts inform individuals that automated processing will take place and establish a legal basis for such processing.

Implications for Private Equity and M&A transactions

Given all of the above, during the diligence process we believe that it will be increasingly important to examine the target's big data analytics activities and determine whether the target has carried out any DPIAs. The inadequacy (or absence) of a robust data governance framework could be a red flag particularly in data heavy sectors such as Fintech, healthcare, insurance, technology, financial services and retail.

Key Takeaways:

Organisations are becoming increasingly cognisant of the risks associated with data analytics, and are looking to implement effective data governance and management structures. These risks are most prevalent in data heavy sectors such as Fintech, healthcare, insurance, technology, financial services and retail.

Automated data processing presents great opportunities to enhance business agility and efficiency, but can conflict with the underlying principles of the GDPR and other privacy laws. This means that decisions which are solely based on automated processing which legally affect individuals are restricted.

The consequences of non-compliance with data protection regulations are becoming ever more severe. The regulatory landscape is continually evolving, creating a more complex framework for organisations to navigate. In addition to high regulatory fines, some organisations which have been affected by data breaches are contending with class action claims. Organisations also risk

reputational damage and a loss of trust.

Data governance should be a key diligence item. Potential buyers will increasingly need to assess management's awareness of the risks associated with their data analytics activities and understand whether the target has in place appropriate governance and protocols.

If you would like more information about the topics raised in this briefing, please speak to your regular contact at Weil or to any member of the Cybersecurity, Data Privacy & Information Management Group.

Barry Fishley	View Bio	barry.fishley@weil.com	+44 20 7903 1410
George Mole	View Bio	george.mole@weil.com	+44 20 7903 1367