Reconciling innovation and regulation: mission impossible?

Can big data coexist in harmony with data protection law? Fiona Maclean and Olga Phillips, Associates at Latham & Watkins, explore

As the technology sector continues to grow in prominence in nearly all industries, and data protection law becomes more regimented and widespread, the debate around the compatibility of innovation and big data with data protection law is increasingly pertinent. In 2015, the EU's Digital Single Market Strategy cited big data as being 'central to the EU's competitiveness', and a 'catalyst for economic growth'. Many critics argue that big data will never coexist in harmony with data protection law, and that it is ultimately big data *versus* data protection law, rather than big data *and* data protection law. However, organisations and regulators are rising to the challenge by developing innovative processes and technologies that both meet regulatory standards and, in some cases, provide a mechanism for complying with laws.

So, how do organisations looking to deploy innovative technologies meet consumer expectations without crossing that uncomfortable line? And how can they leverage the resulting big data within the framework of the General Data Protection Regulation ('GDPR') and other data protection laws?

Consumer expectations and big data

The capabilities of big data are innumerable; big data can identify infectious diseases, protect online banking information, and detect fraud.

The UK Competition and Markets Authority ('CMA') emphasises that big data can produce a 'wide range of benefits' for consumers such as 'more personalised services, greater choice and more relevant advertising'. Increasingly, consumer-facing sectors, for example, retail and financial services, are using new technologies to offer consumers a different customer experience, such as artificial intelligence and robo-advisors, connected stores, and the Internet of Things. In many cases, consumers unknowingly use big data solutions and find that they appreciate the way big data simplifies their day-to-day lives, such as when an online store remembers the contents of a consumer's shopping cart, or presents personalised promotions and recommendations. Consumers therefore generally support the development of these technologies, and have a reasonable expectation that organisations will deploy them in some manner.

However, in some cases innovation and big data have attracted bad press, highlighting the sometimes uncomfortably far-reaching capabilities of this technology. For example, a major American retailer reportedly knew a customer was pregnant before she had had the chance to tell her own family.

Privacy by Design and Default

At the outset, Privacy by Design (the subject of the article appearing on pages 3-6 of this edition) is one of the core tools organisations have to ensure that the use of big data analytics does not come at the cost of privacy. The principle of Privacy by Design places the onus of ensuring privacy back squarely with the controller. Controllers cannot merely rely on data subject consent to justify their use of data sets; rather, controllers must take pre-emptive measures to protect privacy by conducting ex ante impact assessments.

Embedding Privacy by Design principles into the development of innovative technology solutions serves to remind developers and employees of the importance of protecting the underlying data and, in some cases, is now a legal requirement under the GDPR. For example, Article 35 of the GDPR states that if a type of processing uses new technologies that may result in processing that poses a high risk to the rights and freedoms of natural persons, the controller should undertake a data protection impact assessment ('DPIA').

The UK's Information Commissioner's Office ('ICO') report 'Big data, artificial intelligence, machine learning and data protection' ('ICO Big Data Report'), recognised that, in the context of big data analytics, conducting DPIAs can be challenging. However, the report also acknowledged that DPIAs are a necessary step in identifying associated privacy-related risks, and essential when relying on legitimate interests as the purpose for processing big data.

Consider potentially less privacy-intrusive methods

The DPIA may, of course, highlight that organisations must consider alternative, less privacy-intrusive methods of obtaining the same objective.

In the ICO Big Data Report, the regulator noted that anonymisation should not be overlooked as a significant compliance tool in the use of big data analytics. Anonymising personal data takes processing outside the scope of the GDPR, and significantly minimises the risks associated with processing such data. The ICO implores organisations to consider whether identifying specific individuals is necessary to achieve the objective of their analytics. For example, when using location data from mobile phones to track the movement of crowds of people, or to assess how many people use trains at a particular time, the identity of the individuals involved is not necessarily required to analyse the results.

> *"In the ICO Big Data Report, the regulator noted that anonymisation should not be overlooked as a significant compliance tool in the use of big data analytics. Anonymising personal data takes processing outside the scope of the GDPR, and significantly minimises the risks associated with processing such data."*

Lawfulness

Where personal data are involved, organisations must consider the legal basis for processing such data. Consent is considered binary, and the often opaque nature of processing big data means meaningful consent is difficult to achieve.

The quantities and categories of personal data that companies process often exceed what the performance of a contract requires, and relying on 'legitimate interests' as a ground for processing requires the interests of organisations to outweigh those of individuals — often a difficult balancing test.

However, the technology industry can help itself. For example, the World Wide Web Consortium has already developed a Platform for Privacy Preferences ('P3P'). This platform allows users to set their privacy preference in their P3P-enabled browsers, and checks the browser settings against a website's privacy policy. In addition, the European Union Agency for Network and Information Security ('ENISA') encourages organisations to explore novel ways to obtain consent, including the use of 'gesture, spatial patterns, behavioural patterns [and] motions' — all of which may be suitable in the context of big data.

Privacy notices

Under EU consumer and privacy laws, transparency is key to compliance. In traditional online stores, transparency is relatively simply achieved — terms of service and privacy policies can be displayed to users at the point of sale. However, when there are multiple sources, and data are inferred and/or collected from hundreds of individuals through a single source, meeting the transparency principle is more problematic.

In some cases, organisations can learn from older technologies that have already overcome this hurdle. A good example is CCTV, which has, over the years, developed a standard icon to alert customers that their image is being collected. In the context of drones, the Irish Data Protection Commissioner ('DPC') has suggested using conspicuous signage, advertising, and leaflets. Notably, the DPC has stated that the dates and times of flights and the flight path should also be included in the privacy notice, suggesting that the controller should consider whether to exceed the GDPR standard in order to ensure transparency.

In the context of more traditional analytics online, such as the use of cookies and web beacons, organisations should ensure that they have detailed, GDPR-compliant privacy policies and that they supplement these policies with appropriate just-in-time notices throughout the customer journey.

Data subject rights

The GDPR gives individuals rights of restriction, access, correction, deletion, and portability (amongst others). Critics suggest that the sheer volume of big data poses a challenge for organisations in fulfilling these obligations, as data are dispersed over hundreds of servers in incomprehensible quantities. Collating these data, which may include unstructured data, within the statutory one-month timeframe — as well as identifying data that have been observed, derived, or inferred about the individual — can prove taxing for organisations.

Once again, organisations can often draw upon other innovative technology solutions to ensure that they comply with this requirement, even in the world of big data. Indeed, the GDPR recommends this approach: Recital 63 states that "[w]here possible, the controller should…provide remote access to a secure system which would provide the data subject with direct access to his or her personal data". In blockchain, for example, self -sovereign identity applications purport to hand control of personal data back to the data subject so that subjects can access and share data at their discretion. Likewise, many social network providers have implemented services that allow users to download their data at the click of a button,

(Continued on page 12)

(Continued from page 11)

providing individuals with copies of their personal data within 48 hours.

How are the regulators responding?

Across various sectors, regulators have recognised that while innovation can bring great opportunities for businesses and consumers alike, it also poses many risks to existing regulatory framework and consumer rights. In the financial services sector, the UK's Financial Conduct Authority ('FCA') has championed the use of innovation and the fostering of competition in financial services since launching Project Innovate in October 2014. The FCA encourages innovation within established legacy firms and supports FinTech startups entering the market. In doing so, the FCA has recognised that big data is a major component of the burgeoning world of FinTech.

Charles Randell, FCA Chair, explored big data ethics in a speech delivered in London in July 2018. Randell stated that people must remain at the centre of a firm's purpose and governance and that individuals, rather than machines, must ultimately be accountable for whether the outcomes of certain processing activities are ethical. In a similar vein, the ICO has stated that "the world of data protection and data ethics are not sitting in separate universes". Furthermore, the European Commissioner for Competition, Margrethe Vestager, has stressed that data pooling and sharing is welcome provided it recognises privacy.

Regulators have responded to the challenge of balancing the use of big data with ethical processing. Both the ICO and the FCA have publically supported the UK government's development of the Centre for Data Ethics and Innovation. The centre is tasked with developing 'overarching ethical principles for AI' in conjunction with the recently established AI Council and Office for AI.

The CMA also announced recently that it will establish a data unit to investigate digital competition law issues, including the use of algorithms, big data, and machine learning.

The CMA's data unit will investigate the effect big data may have on consumer relationships, and seek to assess whether such effects are both ethical and in the consumer's interests.

Regulators perceive their role in overseeing the use of big data as active, not passive. This is evident in the growing number of regulatory sandboxes offered by the FCA, ICO, and other global regulators, providing safe-havens in which organisations can test new products in controlled environments.

Regulators are active in encouraging and monitoring the development of technology and how organisations within their regulatory control use big data. This increased regulatory scrutiny is a positive milestone for both organisations and consumers.

As the use cases grow and organisations increasingly adopt more innovative technology, we will likely see more regulatory activity, and possibly industry standards, codes of practice, and even new laws in the not-too-distant future.

Conclusion

Evidently, big data presents challenges to the traditional application of data protection law. Provided that organisations are considerate of their privacy obligations, and keep consumer rights and freedoms at the forefront of their minds, innovative uses of data and the concepts of privacy and data protection can conceivably work in harmony.

However, big data, AI, and machine learning are fast-moving and, as a result, regulators will most likely always be one step behind. Organisations must be cognizant of this possibility and think carefully about their deployment of data-centric processes and technologies. Companies should self-regulate their own activities while the regulators continue to educate themselves on the expanding role of big data analytics across consumer-facing sectors. Trust, and therefore transparency, are fundamental to ensuring that big data has a real (and positive) future in society. Consumers must feel confident that, while the technological uses for personal data may be endless, businesses have not lost sight of the people behind the online world.

Fiona Maclean and Olga Phillips
Latham & Watkins
fiona.maclean@lw.com
olga.philips@lw.com