MORRISON | FOERSTER

Morrison & Foerster Client Alert

November 14, 2014

Big Data Series: Part 1: Privacy - "Big Data is not a game played by different rules"

By Sue McLean, Ann Bevitt, Karin Retzer and D. Reed Freeman

Big data is now big business. In recent years, due to the exponential growth in the capability of technology to undertake data analytics on a massive scale, organisations have started to appreciate the potential hidden value that could be derived from their data. In March 2014, Neelie Kroes (Vice President of the EU Commission responsible for the Digital Agenda) reflected this view when she hailed a "*data gold rush… a new industrial revolution… a digital revolution fuelled by big data*".

It's certainly clear that big data analytics can drive potential significant benefits. Information produced from analytics can help companies to forecast and make better decisions, make savings and efficiencies, and improve agility. However, big data can also produce significant legal risks, in particular, in terms of data privacy and security. In this first Alert in our Big Data Series, we highlight how different data protection authorities around the world are addressing big data and discuss how organisations can best manage their privacy compliance when embarking upon big data projects.

WHAT IS BIG DATA?

Organisations have always accumulated information but, in this digital age, the amount of data being generated and retained is growing exponentially. IBM has calculated that 90% of the digital data that exists today was created in the last two years. In addition, historically, organisations may not have been able to draw value from the data that they held, particularly where such data was unstructured (and Gartner estimates that roughly 80% of all corporate data is unstructured). However, new technologies now enable the analysis of large, complex and rapidly-changing data sets comprised of structured, semi-structured or unstructured data. In short, "big data" is just data. It's simply that we have more of it and we can do more with it.

UNITED STATES	
California	
Tiffany Cheung	(415) 268-6848
Peter Day	(650) 813-4231
Rebekah Kaufman	(415) 268-6148
Christine E. Lyon	(650) 813-5770
David F. McDowell	(213) 892-5383
Purvi G. Patel	(213) 892-5296
Andrew Serwin	(858) 720-5134
William L. Stern	(415) 268-7637
Nancy R. Thomas	(213) 892-5561
David M. Walsh	(213) 892-5262
New York	
Cindy Abramson	(212) 336-4178
Melissa Crespo	(212) 336-4354
John F. Delaney	(212) 468-8040
Michael B. Miller	(212) 468-8009
Sotirios Petrovas	(212) 336-4377
Suhna N. Pierce	(212) 336-4150
Marian Waldmann Agarwal	(212) 336-4230
Miriam H. Wugmeister	(212) 506-7213
Washington, D.C.	
Patrick Bernhardt	(202) 887-8771
L. Richard Fischer	(202) 887-1566
Adam J. Fleisher	(202) 887-8781
D. Reed Freeman, Jr.	(202) 887-6948
Libby J. Greismann	(202) 778-1607
Julie O'Neill	(202) 887-8764
Cynthia J. Rich	(202) 778-1652
Nathan David Taylor	(202) 778-1644
EUROPE	
Berlin	
Hanno Timner	49 30 72622-1346
Brussels	
Karin Retzer	32 2 340 7364
Alja Poler De Zwart	32 2 340 7360
London	
Ann Bevitt	44 20 7920 4041
Amy Collins	44 20 79204180
Susan McLean	44 20 79204045
ASIA	
Beijing	
Gabriel Bloch	86 10 5909 3367
Jingxiao Fang	86 10 5909 3382
Paul D. McKenzie	86 10 5909 3366
Hong Kong	
Gordon A. Milner	852 2585 0808
Singapore	
Daniel P. Levison	65 6922 2041
Tokyo	
Toshihiro So	81 3 3214 6568
Yukihiro Terazawa	81 3 3214 6585

BIG DATA IN EUROPE

Over the summer of 2014, the UK's data protection regulator, the Information Commissioner's Office ("ICO"), held a public consultation on its report on "Big Data and Data Protection" ("ICO Report"). The consultation ended on 17 October 2014 and the results are awaited.

The ICO Report is the first specific guidance on big data issued by a European data protection authority. At a European level, the Article 29 Working Party (a group composed of the national data protection authorities (DPA), the European Data Protection Supervisor and the European Commission), has issued various opinions that are relevant to big data (including in terms of anonymisation, purpose limitation and legitimate interest), but has not yet issued specific guidance on big data.

In June 2014, the Article 29 Working Party stated that it does not believe that data protection principles are challenged by big data, but intends to carry out a comprehensive assessment of big data and release its analysis. It's also worth noting that, when adopted, the new EU Data Protection Regulation is likely to introduce additional requirements in the context of big data analytics, in that the Regulation aims to improve transparency, enhance individual rights and introduce wider use of "privacy by design" and privacy impact assessments.

KEY FINDINGS OF ICO REPORT

The main message of the ICO Report is the not-exactly-surprising conclusion that "big data is not a game played by different rules". The UK Data Protection Act 1998 still applies to the processing of personal data for the purposes of big data analytics.

Some of the ICO Report's other, more helpful, key findings are as follows:

- **Transparency**. In order to ensure fairness in processing, organisations need to be transparent when they collect data and explain how such data are used. The complexity of big data analytics is not an excuse for not informing users. The ICO states that the fact that most people don't read privacy notices doesn't mean that individuals are not concerned about how their data are used. It may indicate that, from previous experience, they do not expect a privacy notice to give them useful information in an understandable form. Organisations should find innovative ways of conveying the required information in a concise way, *e.g.*, by way of a video. Organisations should consider in-product and just-in-time notices because research shows that people's willingness to give personal data, and their attitude to the use of such data, are context-specific. Organisations should tell people how they are using their data, but they should also tell them when personal data are not being used, *e.g.*, when anonymised data are being used. The ICO believes that this could help dispel some of the mystery surrounding big data and build trust in the use of analytics.

- **Condition for processing**. Big data processing must satisfy one of the conditions for processing such as consent or legitimate interests. In terms of legitimate interests, it's a balancing exercise between the interests of the companies and the rights of the individuals. Furthermore, the processing must be "necessary" for the legitimate interests. "Necessary" is a strict test, *i.e.*, processing won't be necessary if there's a less privacy-invasive alternative. If consent is required, the complexity of big data analytics is no excuse for not obtaining consent. Organisations must find an appropriate point to explain the benefits of the analytics, provide users with a choice and then respect that choice. Consent must be freely given, specific and informed.

- **Using third-party data sets**. If an organisation is using data obtained from third parties, it needs to consider whether it can use that data in anonymised form. If not, it will need to ensure that it has the right to process the data for the required purpose and, if not, provide the appropriate privacy notices to individuals and obtain the necessary consents.

- **Purpose Limitation**. Big data can involve re-purposing personal data, *i.e.*, an organisation collects data for one purpose and wants to start analysing the data for a different purpose. If an organisation is going to re-purpose in this way, then the new purpose must not be incompatible with the original purpose. However, this does not mean that the new purpose must be the same as the old purpose. If an organisation intends to re-purpose data, it must make users aware of this upfront, particularly where the new purpose is not obvious. In the ICO's view, the key factor is whether the processing is fair, *i.e.*, how does the new purpose affect a user's privacy and would it be within the user's reasonable expectations that his or her data could be used that way? If not, then in most cases the organisation will need to seek specific consent.

- **Anonymisation**. The ICO suggests anonymising data, where appropriate. If done correctly, this means that the data are no longer considered personal data and would not be subject to data protection obligations. However, the ICO recognises that, in the context of big data analytics, effective anonymisation can be challenging, and organisations must carry out robust risk assessment. In the ICO's view, the requirement is not to eliminate the risk of re-identification completely, but to ensure that the risk of re-identification can be mitigated so that it is extremely remote. Technical measures such as data masking, pseudonymisation, aggregation, banding, and legal and organisational safeguards should be considered, as further detailed in the ICO's anonymisation code.

- **Minimisation and Retention of Data**. Organisations need to be able to articulate at the outset why they need to collect and process data. They need to satisfy themselves that the data are relevant and not excessive in relation to that aim. In terms of retention, concern has been raised that big data analytics may encourage organisations to retain data longer than necessary just in case the data may prove to be useful in the future. However, the ICO finds no evidence to support this. In the ICO's view, even though the cost of storage is falling, it still represents an overhead that organisations will want to minimise.

- **Security**. The ICO states that it's too simplistic to say that the use of big data increases or mitigates security risk, particularly as there is some evidence that big data analytics can be used to improve information security (*e.g.*, by detecting patterns and anomalies to identify security threats). In terms of security, organisations should be proactive in considering any information security risks posed by big data and apply appropriate safeguards.

- **Ethical Approach**. The ICO recommends taking an ethical approach. Not only will it help businesses show data subjects that they are responsible and trustworthy it will also help with data protection compliance.

BIG DATA IN THE U.S.

In the U.S., there are no laws or regulations specifically targeting big data analytics. (The Fair Credit Reporting Act is a sector-specific law aimed at the use of data sets for the purpose of making eligibility determinations regarding consumers for credit, employment or insurance). If organisations want to embark on big data projects involving personal data, they need to ensure compliance with applicable privacy laws, including, most importantly, Section 5 of the FTC Act, which prohibits unfair and deceptive acts and practices. To that end, the FTC has stated that uses of data unlikely to be reasonably anticipated by consumers under the circumstances (so-called “secondary uses”) may require “enhanced” notice, i.e., notice outside of the privacy policy and displayed prominently for the user. The FTC also believes that big data carries serious data security concerns for the very reason businesses want to use big data: the implications that big data allows a user to draw regarding consumers whose data are included.

To date in the U.S., the specific legislative focus and regulatory response to big data and the rhetoric around big data have been primarily on data brokers. To that end, in May 2014, the White House published a report examining big data and privacy. After closely studying nine data brokers, the FTC also published a report entitled, “Data Brokers: A Call for Transparency and Accountability” in May 2014. In December 2013, the Senate Commerce Committee Staff also published its own report, entitled, “A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes.” The three reports shed light on data brokers’ practices and made various recommendations, including in some cases recommendations to expand U.S. privacy laws, but so far there has been no significant progress in implementing those recommendations in terms of new legislation or regulation.

THE VIEW FROM MAURITIUS

International data protection and privacy authorities met for a closed session from 13 – 16 October 2014 at the 36th International Conference of Data Protection and Privacy Commissioners in Mauritius. In the Resolution Big Data issued after the conference, the group of regulators noted that big data entails a new way of looking at data, thereby revealing information which may have been previously difficult to extract or otherwise obscured. More extensive use of big data is likely to have adverse consequences for the protection of privacy and other fundamental rights. The regulators therefore called upon all parties making use of big data to:

- respect the principle of purpose specification (*i.e.*, process data only for the purposes for which data were collected and individuals were notified of and consented to);
- limit the amount of data collected and stored to the level that is necessary for the intended lawful purpose;
- obtain a valid consent from data subjects;
- be fully transparent (provide clear privacy notices);
- give individuals appropriate data access and correction rights;
- give individuals access, where appropriate, to information in a clear and understandable format about the key inputs and the decision-making criteria (algorithms) that have been used as a basis for development of a profile;
- carry out a privacy impact assessment, especially where the big data analytics involves novel or unexpected uses of personal data;
- develop and use big data technologies according to the principles of privacy by design;
- consider data anonymisation on a case-by-case basis, possibly using a combination of anonymisation techniques;

  - exercise great care, and act in compliance with applicable data protection legislation, when sharing or publishing pseudonymised, or otherwise indirectly identifiable, data sets; and
  - demonstrate that decisions about the use of big data are fair, transparent and accountable and continue assessment of the underlying algorithms and profiles of data used for profiling purposes.

MANAGING BIG DATA

When implementing big data analytics projects, organisations need to address data protection compliance and implement appropriate policies and procedures. In particular:

- they need to start with the basics: understand what personal data the organisation has, where the data are stored or processed, and what the organisation is permitted to do with the data. If personal data are collected and used for different purposes throughout the business, the organisation needs to understand the data "lifecycle", who is responsible for the data at each different stage. If third-party players are involved, the organisation needs to ensure that appropriate contractual arrangements are in place;
- ensure that the organisation has suitably qualified resources to identify the objectives and parameters of the big data project and analyse the data. To make the most of big data analytics, it can't be considered just an IT or legal issue. The organisation should put in place an appropriate multi-disciplinary team across the key stakeholder teams within the business. In addition, legal advisers (whether internal or external) should be involved early on to ensure that privacy compliance is considered from day 1;
- for each big data project, the organisation should consider all relevant privacy issues, for example:
  - consider whether it needs to use personal data at all, or whether it could use anonymised data for its purposes;
  - identify whether it is using analytics to identify general trends or make decisions that affect individuals;
  - ensure that it has a legal basis for processing;
  - if it's using data sets obtained from third parties, check the source and integrity of those data sets. The organisation should ensure that it carries out appropriate due diligence (and, again, ensure that it fulfils one of the appropriate data protection conditions for processing);
  - if it is re-purposing, consider whether the new purpose is incompatible with the original purpose or whether new consent is required;
  - be as specific and transparent as possible with data subjects. The organisation should explain its purposes (particularly where purposes may not be obvious), and the implications and benefits of the processing. It should avoid descriptions that are too vague or general, provide granular information and use layered notices; and
  - put in place appropriate security measures (both physical and logical, *e.g.*, encryption, access management, training, processes and procedures, etc.).

But it's not just a question of compliance with applicable data protection rules. There are also issues of ethics and trust that organisations should consider, as highlighted in the ICO Report. Consistent with the principle of accountability, organisations should try to put themselves in the position of the data subject and consider not just "can we do this?", but "should we do this?" (what some commentators have dubbed the "creep factor".)

CONCLUSION

As the ICO indicates in the ICO Report, privacy by design is not a zero sum game. Privacy compliance shouldn't be seen as merely a negative hurdle to overcome. The public is increasingly concerned about how its data are used (and misused). If an organisation can demonstrate that it takes its data privacy obligations seriously, there can be valuable business benefits. Indeed, as we have recently seen with the meteoric rise of the social media platform, Ello, being seen as privacy-friendly can help an organisation to differentiate itself from its competitors.

In addition, organisations need to bear in mind that privacy is not the only issue to be considered when embarking on a big data project. And, of course, as the ICO Report recognises, there are many instances of big data analytics that do not involve personal data at all. There are various other legal issues that organisations may need to consider, including:

- Compliance with applicable laws and regulations (whether context-specific, or industry-specific)
- Intellectual Property Rights
- Ownership of data
- Contracts with third-party providers
- Competition
- Security
- Consumer Protection
- Liability

We will consider some of these issues further in subsequent Alerts in this Series.

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's A-List* for 11 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "*Global Employee Privacy and Data Security Law*," or our free online Privacy Library, please visit: http://www.mofo.com/privacy--data-security-services/ and follow us on Twitter @MoFoPrivacy.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.