ICDPPC
International Conference of Data
Protection & Privacy Commissioners
Executive Committee

Big Data, Key Challenges: Privacy Protection & Cooperation

Observations on international efforts to develop frameworks to enhance privacy while realising big data's benefits

Seminar arranged by the Office for Personal Data Protection, Macao, China, 2 December 2015

Notes for an address by John Edwards, New Zealand Privacy Commissioner and Chair, Executive Committee, International Conference of Data Protection and Privacy Commissioners (ICDPPC)

Summary

The accumulation and use of 'Big Data' carries both significant challenges for privacy protection and the promise of substantial benefits for society and consumers. It is a topic that has been debated at the International Conference of Data Protection Commissioners in the past and, given the rapid developments in this context, will no doubt be discussed again in the future. John Edwards, the Chair of the Executive Committee of the International Conference, will highlight the Conference's 2014 'Resolution on Big Data' and survey a few examples at national and international level of attempts to develop frameworks to enhance privacy while realising big data's benefits.

Introduction

It is my honour to offer these remarks in my capacity as Chair of the International Conference of Data Protection and Privacy Commissioners rather than as New Zealand Privacy Commissioner – my day job.

It is often suggested that the ability to store and analyse vast quantities of data may prove beneficial to society.

Big Data may be used, for example, to predict the spread of epidemics, uncover serious side effects of medicines and combat pollution in large cities.

But Big Data may also be utilised in ways that raise important concerns with regard to the privacy of the individuals and civil rights, protections against discriminatory outcomes and infringements of the right to equal treatment.

Big Data entails a new way of looking at data, revealing information which may previously have been difficult to extract or otherwise obscured. To a large extent, the privacy debates about ‘Big Data’ involve questions of *reuse* of personal information, often information generated as a by-product of other transactions. This transactional information may be especially valued if it can be used to establish correlations that may help to make predictions about the future.

In New Zealand, one government agency has been exploring the possibility of analysing existing social welfare data to predict the likelihood of harm to vulnerable children. The use of predictive risk modelling is extremely controversial. When children are removed from their families on the basis of a perceived risk threshold, it is impossible to know when we get it wrong and the child and their family’s privacy has been irreparably harmed.

That’s one example of how Big Data can be perceived to challenge key privacy principles, in particular the principles of purpose limitation and data minimisation.

The protection provided by these principles may seem, to many privacy authorities, to be more important than ever at a time when the amount of information collected about us seems every increasing.

But you will sometimes hear commentators say that it is impossible to enforce traditional privacy principles in an age characterised by Big Data and indeed that it is undesirable to do so.

These commentators will instead urge that attention be paid to regulation of the fairness of the final use of information with respect to individuals.

I suspect that wherever you sit in terms of regulation in your own jurisdiction, you will find some merit on both sides of the arguments about the use and reuse of Big Data.

I offer no settled conclusions but want to instead highlight some interesting national and international endeavours to develop frameworks to enhance privacy – all this while realising big data's benefits.

Given the theme of the seminar I highlight aspects of both 'protection' and 'cooperation'.

New Zealand exploration of the issues

I want to begin by mentioning a local endeavour that has informed my thinking and may have something to offer to other jurisdictions internationally.

In 2014, the New Zealand Government set up a working group to advise ministers on how the collection, sharing and use of business and personal information would impact on public services in the coming years.

The New Zealand Data Futures Forum undertook an open process to identify and explore the issues associated with Big Data. The Forum concluded that the way forward needed to focus upon four key concepts:

1. VALUE

2. INCLUSION

3. TRUST

4. CONTROL

I expect that this insight will likely carry through into any jurisdiction and context.

Exploration of the issues amongst privacy authorities

International cooperation and protection often starts by talking together and writing down points of agreement and disagreement.

Amongst privacy authorities, two examples of this are the International Working Group on Data Protection in Telecommunications (known as IWGDPT or the 'Berlin Group') and, of course, the International Conference of Data Protection and Privacy Commissioners itself.

The IWGDPT has looked at Big Data in depth and adopted an 18 page working paper in 2014.[1] Its recommendations focus upon:

- Consent.
- Procedures for robust anonymisation.
- Greater transparency and control from collection to use of data.
- Privacy by Design and Accountability.
- Enhancement of knowledge and awareness.

The International Conference adopted its Resolution on Big Data in October having received the benefit of the Berlin Group analysis.

The two page resolution offered numerous recommendations and include a call to all parties making use of Big Data:

- To respect the principle of purpose specification.

[1] IWGDPT, Working Paper on Big Data and Privacy principles under pressure in the age of Big Data analytics, May 2014, http://www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf?1407931243

- To limit the amount of data collected and stored to the level that is necessary for the intended lawful purpose.

- To obtain, where appropriate, a valid consent from the data subjects in connection with use of personal data for analysis and profiling purposes.

- To be transparent about which data is collected, how the data is processed, for which purposes it will be used and whether or not the data will be distributed to third parties.

- To give individuals appropriate access to the data collected about them and also access to information and decisions made about them. Individuals should also be informed of the sources of the various personal data and, where appropriate, be entitled to correct their information, and to be given effective tools to control their information.

- To give individuals access, where appropriate, to information about the key inputs and the decision-making criteria (algorithms) that have been used as a basis for development of the profile. Such information should be presented in a clear and understandable format.

- To carry out a privacy impact assessment, especially where the big data analytics involves novel or unexpected uses of personal data.

- To develop and use Big Data technologies according to the principles of Privacy by Design.

- To consider where anonymous data will improve privacy protection. Anonymisation may help in mitigating the privacy risks associated with big data analysis, but only if the anonymisation is engineered and managed appropriately. The optimal solution for anonymising the data should be decided on a case-by-case basis, possibly using a combination of techniques.

- To exercise great care, and act in compliance with applicable data protection legislation, when sharing or publishing pseudonymised, or otherwise indirectly identifiable, data sets. If the data contains sufficient detail that is, may be linked to other data sets or, contains personal data, access should be limited and carefully controlled.

- To demonstrate that decisions around the use of Big Data are fair, transparent and accountable. In connection with the use of data for profiling purposes, both profiles and the underlying algorithms require continuous assessment. This necessitates regular reviews to verify if the results from the profiling are responsible, fair and ethical and compatible with and proportionate to the purpose for which the profiles are being used. Injustice for individuals due to fully automated false positive or false negative results should be avoided and a manual assessment of outcomes with significant effects to individuals should always be available.

Finally, before moving beyond attempts by privacy authorities to explore the Big Data issues and document recommended practices, I should mention that the EU authorities adopted a joint statement in September 2014.[2]

Its 14 ‘key messages’ may be said, at their heart, to contain a message that the legal controls applicable in Europe are required to be adhered to including in the context of processing of big data.

Putting principles into practice

Finally, I offer one example of an attempt by an international organisation involved in Big Data analytics to actually attempt to implement a privacy framework to enhance privacy while realising big data’s benefits.

Global Pulse is a United Nations innovation initiative that explores how new, digital data sources and real-time analytics technologies can provide a better understanding of changes in human well-being and emerging vulnerabilities.

[2] Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU, September 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf

However, legitimate concerns about privacy and data protection present challenges to harnessing Big Data sets for public benefit.

Global Pulse states that it respects and values individuals' privacy and protecting it forms the cornerstone of our work. Accordingly, in consultation with privacy experts, Global Pulse has developed a set of Privacy Principles.

Those principles are expressed as follows:

> *We access, analyse, store, transmit or otherwise use only data that has been obtained by lawful and fair means, including, where appropriate, with the knowledge or consent of the data subject*
>
> *We do not access data containing personal information on any individual, without the knowledge or proper consent of the data subject*
>
> *We never access the content of private communications, without the knowledge or proper consent of the data subject*
>
> *We never attempt to re-identify anonymised data, without the knowledge or proper consent of the data subject*
>
> *We will only access, analyse, store, transmit or otherwise use data in accordance with the purposes for which the data has been properly and lawfully obtained*
>
> *We ensure reasonable and appropriate technical and organisational safeguards are in place to prevent unauthorised disclosure or breach of data*
>
> *We design, carry out, report and document our activities with accuracy and transparency*
>
> *We employ even stricter standards of care while conducting research among vulnerable populations and persons at risk, children and young people, and any other sensitive data*

> *We perform due diligence when selecting data or service provider partners and ensure their activities comply with the United Nations' global mandate*
>
> *We ensure that our research partners are acting in compliance with relevant law, privacy and data protection standards*

Global Pulse has established a Data Privacy Advisory Group[3] comprised of experts from public and private sector, academia and civil society, as a forum to engage in a continuous dialogue on critical topics related to data protection and privacy with the objective of unearthing precedents, good practices, and strengthen the overall understanding of how privacy protected analysis of big data can contribute to sustainable development and humanitarian action.

Several privacy commissioners - or their staff - have accepted appointment to this advisory group.

A major project Global Pulse is currently embarked upon is revising and road testing a Privacy Impact Assessment template – a methodology expressly recommended in the International Conference resolution.

Closing comments

In this brief survey I have highlighted a few examples of international cooperation in the addressing the privacy challenges of big data while reaping the benefits.

I end on a summary version of one of the key recommendations of the New Zealand Data Futures Forum:

> Establish the foundations: value, inclusion, trust and control

ENDS

[3] http://www.unglobalpulse.org/data-privacy-advisory-group