BIG DATA, BIG ISSUES?

IS AUSTRALIAN PRIVACY LAW KEEPING UP?

By Reyhaneh Saadati, Solicitor & Alec Christie, Partner, DLA Piper

Big Data has been dubbed by many as the "new economic asset" of our age and of potentially significant value to business.

Following the recent amendments to the *Privacy Act* and in anticipation of his new powers from 12 March 2014, the Australian Privacy Commissioner Timothy Pilgrim (**Commissioner**) advised Australians earlier this year that "*2013 is shaping up to be the biggest year for privacy in over 20 years*".[1]

Even though the recent amendments to the *Privacy Act* and the new Australian Privacy Principles (**APPs**) do not specifically address the Big Data technology/regulation gap, discussions by and between business, individuals, the media and even the Commissioner about Big Data have recently sparked up.

WHAT IS BIG DATA?

Big Data is the tracking and aggregation of a large volume of data (including personal information) from search engine histories, emails, sales transaction histories, reward/loyalty programs, app downloads and the like.

The aggregation, tracking and analysis of large volumes of data across such a range of variables is of considerable value to business, allowing business to gain insight into its consumers and the market, making it more responsive, increasing efficiency and encouraging new offerings for "new" markets. As well as using their own data, businesses are also finding more and more ways of combining their data with that of third parties (as well as publically available information) in order to analyse more variables and to "slice and dice" the data in more and more ways.

WHAT IS BIG DATA USED FOR?

Analysis of Big Data can be (and is) used to reduce fraud, map disease outbreaks, further scientific research, improve business processes and assist in creating new innovative and wanted products.[2] However, there is also a perceived "dark side" to Big Data, especially where such is considered to be an interference with privacy (whether we know it or not).

The extensive amounts of personal information we reveal as we transact online has taken the relationship between customer profiling, predicting trends and marketing to a whole other level. Big Data is capable of tracking movements, behaviours, preferences and predicting the behaviour of individuals with unprecedented accuracy. The more access business has to Big Data the better they can target us with advertising and products that match (or rather predict) our specific interests. This is, however, often done without our consent.

---

1 With the introduction in May of a Bill introducing mandatory breach notification (although not passed), there can be no doubt of this.

2 See article entitled "*MIT Profs Mull Privacy Concerns as They Parse Big Data*" published in The CIO Report - The Wall Street Journal on 22 May 2013.

WHY ALL THE FUSS?

In a speech given in April 2012 the Commissioner referred to an article by journalist Aleks Krotoski[3] which reported the purchase of the social media start-up Social Calendar[4] by US chain store Walmart. In the article Krotoski points out that, when users of Social Calendar listed friends' birthdays or their holiday details, users would have had no idea that the information they included in Social Calendar would end up in the hands of Walmart. This purchase effectively means that Walmart will, subject to applicable law, be able to cross reference the data from Social Calendar users with its own data to generate profiles of users and their friends (and significant events/celebrations in their lives) for direct marketing opportunities.[5]

Perhaps the most dramatic example of the use of Big Data occurred early last year when Target's analysis of Big Data worked out that a teen girl was pregnant (before her father knew), but did not flag that she was a teen, and sent her direct marketing for baby and maternity products. This incensed the girl's father – was Target trying to encourage his teen daughter to fall pregnant? Of course, Target chose not to analyse the Big Data to determine whether this person was over 18 before sending her this marketing. However, Target's chosen analysis of its Big Data was able to determine that she was pregnant (and therefore a potential customer). By tracking and analysing her spending habits (not just at Target) Target was able to determine (a) she was expecting a baby and (b) how far along with the pregnancy she was, with unsettling accuracy.

Examples such as these make it increasingly clear that there is a gap between what can be done with Big Data and what is currently regulated/what we as consumers are ready for.

THE CURRENT AUSTRALIAN LANDSCAPE

Outside of privacy and spam, Australian law does not currently regulate Big Data. The *Privacy Act* regulates the collection, use and disclosure of information or an opinion about an identified individual or an individual who is reasonably identifiable (**Personal Information**) by imposing certain mandatory notification and consent obligations on entities collecting such information. In addition, the *SPAM Act* prohibits the sending of electronic marketing communications without the prior "opt-in" consent of the recipient.

Identified vs de-identified information

The concepts of Personal Information, de-identified information and the applicability of the *Privacy Act* to Big Data appear, at first glance, simple enough. However, on further consideration, this is not straightforward in the Big Data context: can the information contained in Big Data ever truly (ie permanently) be de-identified?

Big Data has historically been used for tracking the movements and interests of groups in a de-identified form (ie such that it does not identify any individual in the group). Of course, use of de-identified information is not regulated and business is free to collect, analyse and use such data as it sees fit. However in recent years, as the power of Big Data is discovered and the associated analytical tools are developed, there has been an increasing ability to and a trend towards tracking the movements and predicting the interests of identified individuals.

Even if the data is de-identified (ie the business is seeking to track/predict the behaviours of groups rather than individuals), the current (and future) data analysis capabilities are such that aggregation of vast amounts of data and the analysis available across such a vast range of Big Data collected from multiple sources (each of which may be de-identified individually) will almost certainly enable re-identification of the individuals concerned.

Of course, as soon as the information is re-identified (or re-identifiable), the collection, use and disclosure of such will be subject to the obligations of and restrictions imposed on the use of such Personal Information under the *Privacy Act*.

---

3 Article entitled "*Big Data age puts privacy in question as information becomes currency*" published in 'The Guardian' on 22 April 2012.

4 A very popular calendar app on Facebook which allows users to record special events such as the birthdays, anniversaries, etc of family and friends.

5 Of course, this is subject to any consent requirements under the relevant US law.

When are mandatory notice & consent(s) required?

If Big Data held by a business includes Personal Information (including information which is reasonably capable of being re-identified), the *Privacy Act* requires that the relevant individuals from whom the information was collected be provided with mandatory notice regarding certain matters (such as the purpose of collection, use and the types of entities to which it is likely to be disclosed) at or before the time of collection of such information.[6] Also, if any of the information to be collected is sensitive information (such as health records, criminal convictions, race, sexual preference, etc) or if Personal Information is to be used for a purpose other than the primary purpose for which it was collected then prior consent of the individual will be required.[7]

Business usually provides mandatory notice and obtains any necessary consent(s) through its privacy policy and processes at the time the Personal Information is first collected by the business. As part of the process individuals are often required to expressly consent to the privacy policy (including the purposes for collection and any required consents), often by clicking a button or ticking a check-box in order to proceed.

However, in the Big Data context, at the time of original collection of the information which later becomes part of Big Data, the business (even if it has collected all the relevant data itself) is often not aware of the full extent of the potential uses it may have for such Personal Information as part of any future Big Data analysis. In addition, the significant volume of non-identified information collected legitimately without notice to and, sometimes, without the knowledge of the individual (eg via dynamic IP addresses, websites cookies, mobile phone location, etc) may itself become Personal Information when used as part of Big Data, by being combined with other data and analysed in such a way that results in its identification of or connection to a specific individual.

In practice it is expensive and impractical for business to go back to individuals at a future date to re-notify and/or re-consent for the new Big Data purpose(s) or for the "new" Personal Information collected (ie when de-identified information is re-identified). As a result many potential uses of the information, to which individuals may not have objected if asked when first collected, remain "locked-up" or, worse, business will simply ignore the privacy law. Essentially, the failure of regulation to keep pace with technology and the rise and use of Big Data acts as an impediment to commercialisation and technological innovation by business or, at least, a disincentive for business to comply with the privacy law.

Where business does anticipate certain future uses of Personal Information it may need to notify customers of (or require their consent to) either very complex or vague statements in their privacy policies in an attempt to comply with the obligations under the *Privacy Act*. Some customers may be put off by this and simply abandon the purchase of the goods or services, particularly in the online world. Also, individuals who provide consent without actually reading the privacy policy or understanding what they are consenting to, how their information will actually be used and whose hands it may end up in may be "shocked" by use of their Personal Information as part of Big Data analysis and there may be a customer revolt against the business (even though the privacy policy of the business technically notifies such use).

A survey funded by the Australian Research Council identified that more than 60% of respondents rarely or never read website privacy policies.[8] Therefore the use of Big Data for purposes not reasonably expected by customers (particularly in the marketing context), without clear and transparent notice (ie informed consent), will likely result in unfavourable customer sentiment and may significantly increase the risk of a complaint to and investigation (or regulation) by the Commissioner.

Marketing (electronic and traditional)

Under the *SPAM Act* business cannot send electronic marketing communications (such as emails, SMS and MMS) to individuals, even if analysis of the Big Data shows that the individual wants such marketing, without that individual's prior consent.

---

6 Or, if it is not practicable to provide notice at this time, it can be provided as soon as possible after collection.

7 Or a purpose related to the primary purpose.

8 Survey conducted by Mark Andrejevic of the University of Queensland's Centre for Critical and Cultural studies and presented by the Commissioner in Brisbane on 26 April 2012 at the University of Queensland Privacy Seminar.

If the Big Data includes Personal Information (as it likely does in most Big Data circumstances), business is not able to use that Personal Information to send non-electronic (ie traditional hard copy) marketing if the recipients would not reasonably expect to receive such marketing communications.

Where consent is required to use Big Data for marketing initiatives, business is faced with the same consent issues discussed above.

WHERE TO FROM HERE?

Both the *Privacy Act* and the *SPAM Act* were enacted before the rise of Big Data and neither adequately addresses the concerns of individuals or provides clarification for business regarding the steps that should be taken to manage the competing interests (ie balancing the protection of an individual's privacy against the business desire to use this valuable "new economic asset" that is Big Data).

Recently there has been much debate around whether uses of Big Data should be subject to increased or specific regulation. Some commentators have suggested that the use of Big Data should be subject to limitations that cannot be circumvented, even with an individual's consent. Others suggest, more reasonably, imposing "informed consent" obligations similar to the overseas transfer consent obligation in the new APPs (ie that the consequences of consent be specifically spelt out for and notified to individuals). Alternatively, we could see a shifting of the obligation for protecting Personal Information to the business using that information in the Big Data context and a prohibition on business using customer consent to get around those obligations.[9]

The recent amendments to the *Privacy Act* do not specifically address Big Data. In fact, during the Privacy Week 2013 breakfast held in May, the Commissioner spoke of the gap between practice and regulation by stating that, when it comes to Big Data, the consent model under the Privacy Act (including the recent amendments) is under pressure. The Commissioner went on to suggest that the key to overcoming some of the issues in the Big Data space is likely to be transparency.

In light of the views expressed by the Commissioner, we believe it is likely that a guidance document will be issued by the OAIC on Big Data in the near future.

IN THE MEANTIME: PRACTICAL TIPS FOR COMPLIANCE

In the absence of clear regulation or guidance from the OAIC on Big Data at present, business can adopt a number of best practice steps to minimise the risks of infringing the *Privacy Act*/ending up being investigated by the Commissioner following a customer complaint. Specifically, business can:

- Audit existing databases to determine what Personal Information they collect and hold, the purpose of collection and whether they are (or are likely) to track and aggregate such information for marketing purposes or purposes other than for which the information was originally collected. Knowing what you have and how you use it is the first step to compliance.
- Examine the Big Data used and whether information that is not identified separately is "re-identifiable" by combination or through analysis and, if so, review original notices provided and consents obtained at the time of collection of that information.
- Focus on transparency by providing continuous notification each time there is a change in practices around collection, use or disclosure of Personal Information. Such notification should clearly set out the main ways in which the new practices are likely to impact individuals. Although keeping individuals informed will not remedy the shortcomings of the *Privacy Act* in respect of Big Data, greater transparency will (it is hoped) decrease potential customer fall-out from unexpected use of Personal Information as part of any analysis of Big Data.
- Ensure the privacy policy is clear, concise and customer friendly. Mobile websites and apps should contain a short form privacy notice (ideally no longer than one screen shot) which is easy to locate and

9 In submissions to Microsoft in January 2013 the OAIC indicated support for a move towards placing responsibility on data users (ie business) rather than individuals in order to ensure that the expectation of privacy is met, rather than the current approach of simply complying with black letter obligations.

which must be viewed before the customer can submit any Personal Information. The short form privacy notice could contain a functional link to the full privacy policy.

- Adopt continuous and flexible consent regimes where business wishes to use Big Data for marketing activities. For example, require customers to re-consent periodically to ensure their consent is current.
- Consider, in certain circumstances, detangling consents relating to uses of Personal Information which are not essential to the purchase of the goods or services from the remainder of the privacy policy so that customers can choose to consent to essential and non-essential uses separately. In such cases, incentivise the consent for non-essential uses.
- Ensure internal practices with respect to the handling of Personal Information are compliant with the recent guidance documents issued by the OAIC (including the recently issued "Guide to Information Security").[10]

Please do not hesitate to contact either of the authors or other members of our dedicated privacy team if we can assist with the review/audit of your current practices in respect of Big Data or if you require assistance to ensure compliance with the new privacy regime to become effective on 12 March 2014.

10 Please refer to our Previous Update for further details.

CONTACT YOUR NEAREST DLA PIPER OFFICE:

BRISBANE

Level 29, Waterfront Place
1 Eagle Street
Brisbane QLD 4000
T +61 7 3246 4000
F +61 7 3229 4077
brisbane@dlapiper.com

CANBERRA

Level 3, 55 Wentworth Avenue
Kingston ACT 2604
T +61 2 6201 8787
F +61 2 6230 7848
canberra@dlapiper.com

MELBOURNE

Level 21, 140 William Street
Melbourne VIC 3000
T +61 3 9274 5000
F +61 3 9274 5111
melbourne@dlapiper.com

PERTH

Level 31, Central Park
152–158 St Georges Terrace
Perth WA 6000
T +61 8 6467 6000
F +61 8 6467 6001
perth@dlapiper.com

SYDNEY

Level 38, 201 Elizabeth Street
Sydney NSW 2000
T +61 2 9286 8000
F +61 2 9286 4144
sydney@dlapiper.com

www.dlapiper.com

120124069