CLIFFORD
CHANCE

Briefing note September 2016

Big Data, Big Opportunities, Big Privacy

Advertisers and marketers were early adopters of big data analytics and techniques and their uses are becoming critical in non-advertising fields such as artificial intelligence, fintech and biotech.

The increasing use of big data techniques and data sets requires businesses to be diligent about how data is collected, used and stored throughout the entire information lifecycle.

The Office of the Australian Information Commissioner has developed a draft *Guide to Big Data and the Australian Privacy Principles* to assist businesses meet their obligations under the *Privacy Act* 1988 (Cth). We discuss those guidelines in this briefing, to give businesses some assistance with building user trust both in their products and company.

Clifford Chance is the legal sponsor of Deloitte Technology Fast 50 Australia and is proud to support Australia's growing technology companies.

Key takeaways

- Businesses need to be diligent about how big data is collected, used and stored throughout the entire information lifecycle.
- Embed a culture of compliance and "privacy by design". Maintain this culture as the business scales and new products are built.
- Undertake Privacy Impact Assessments to evaluate potential impacts of privacy threats on personal information.
- Use privacy notices and transparent practices as tools to build trust with customers.
- Implement practices and procedures to maintain the quality and security of personal information that is collected.

Big Data

It is well known that big data analytics and techniques have been embraced by advertisers and marketers to identify trends in behaviour and to guide customer acquisition strategies. However, big data is also becoming critical in non-advertising fields such as artificial intelligence, fintech and biotech. Its growth has been driven by increased and accessible computing power and storage as well as technical capabilities to capture large amounts of data through software and sensors. It is rare to find a business which doesn't appreciate the growing influence and opportunities of big data and the harnessing of big data analytics in some way.

The increasing use of big data techniques and data sets requires businesses to be diligent about how data is collected, used and stored throughout the entire information lifecycle. Robust and transparent strategies can have the effect of building user trust, increasing business goodwill and making a company more appealing to investors.

The Office of the Australian Information Commissioner (OAIC) has developed a draft Guide to Big Data and the Australian Privacy Principles (the **Guide**) to assist businesses meet their obligations under the Privacy Act 1988 (Cth) (the Privacy Act). Big data and big data activities may include personal information. The Privacy

Act, which includes the Australian Privacy Principles (APPs), regulates the manner in which personal information is managed, collected, dealt with and maintained.

Management Frameworks and Impact Assessments

A key message from the Guide is that the OAIC encourages businesses to implement an overarching Privacy Management Framework and to conduct Privacy Impact Assessments (PIAs) when developing or reviewing a project that uses big data. This includes new product developments or marketing campaigns.

At its simplest, a Privacy Management Framework provides the following steps for businesses to meet their obligations:

- **Step 1: Embed** a culture of privacy that enables compliance. This involves a 'privacy by design' attitude to culture, systems and initiatives, so that businesses develop projects with privacy designed into the project or product, rather than being added on afterwards.
- **Step 2: Establish** robust and effective privacy practices, procedures and systems.
- **Step 3: Evaluate** privacy practices, procedures and systems to ensure continued effectiveness. Learn from big data activities, privacy complaints, breaches and customer feedback.
- **Step 4: Enhance** responses to privacy issues. Be proactive to continually improve privacy processes and anticipate future challenges.

PIAs are used to identify the way a project may impact an individual's privacy. They also assist with the implementation of risk mitigation strategies to manage data and minimise the likelihood and impact of data breaches. PIAs should be used to assess privacy risks throughout the information lifecycle – collecting, using or disclosing and maintaining information.

De-identifying personal information

Generally, data that is de-identified is no longer considered to be personal information and the Privacy Act will not apply. The de-identification of personal information may occur during various stages of big data activities such as when the personal information is initially collected, prior to big data analytics, or prior to the results being published. Businesses may adopt de-identification techniques such as aggregation, using pseudonyms, redaction or making small changes to the data set. Whether de-identification is practical for big data will depend on the nature of the personal information, the choice of de-identification techniques available and whether the results will be used or disclosed for internal or external purposes.

Act now

Although the Guide is not legally binding, the OAIC has stated its intention to refer to the Guide when carrying out its functions under the Privacy Act. The non-prescriptive nature of the APPs and the ability for businesses to undertake reasonable steps affords businesses a degree of flexibility in tailoring their personal information handling practices to protect personal information privacy and, importantly, achieving business objectives such as user acquisition and scale.

Key privacy considerations

The Guide provides businesses with concepts and tools to be adopted when developing strategies to ensure that big data activities comply with the APPs. Some key matters that businesses should consider when engaging in big data activities include:

- Personal information must be collected directly from the individual unless it would be unreasonable or impracticable to do so.
- When big data analytics leads to the creation of new categories of personal information from information previously held by the business, the business needs to consider whether it could have solicited and collected the personal information.
- Where information is collected from a third party, the business should make sure that the third party complies with its privacy obligations and that the individual is given appropriate notice.
- A business may solicit and collect personal information that is reasonably necessary for the functions or activities of the business. This may pose some difficulties for the big data concept of using "all the data" for "unknown purposes".

  Provide customers with a privacy notice which clearly sets out information about collection, uses and disclosures of the personal information. This can also be used as a tool to build trust with customers.
- Consider innovative approaches to privacy notices such as "just-in-time" notices, video notices and privacy dashboards.
- Use or disclose personal information only for the primary purpose for which it was collected. Secondary purposes are permitted with consent or when the customer would reasonably expect the business to use or disclose the information for secondary purposes.

  Businesses that intend to disclose personal information to an overseas recipient, for example, by engaging an overseas cloud service provider to store big data, should conduct a detailed assessment of the service provider's privacy policy to ensure that the provider does not breach any APPs in relation to that information.
- Ensure that any personal information that the business collects, uses or discloses is accurate and complete. Given the nature of big data, a business may need to carry out rigorous steps to ensure the quality of personal information.
- Implement an appropriate security framework to protect personal information from misuse, interference, unauthorised access, modification or disclosure and assess the potential impact of a security breach.
- Implement an appropriate security framework to protect personal information from misuse, interference, unauthorised access, modification or disclosure and assess the potential impact of a security breach.
- Destroy or de-identify personal information the business holds once the personal information (including archived copies) is no longer needed for the primary purpose of its collection.

Contacts

Lance Sacks
Partner
T: +61 2 8922 8005
E: lance.sacks@cliffordchance.com

Jerrem Ng
Senior Associate
T: +61 2 8922 8069
E: jerrem.ng@cliffordchance.com

Catherine Lo
Graduate Lawyer
T: +61 2 8922 8026
E: catherine.lo@cliffordchance.com

Justin Harris
Partner
T: +61 8 9262 5503
E: justin.harris@cliffordchance.com

Shane Stewart
Senior Associate
T: +61 8 9262 5507
E: shane.stewart@cliffordchance.com

#500986-4-10069

Clifford Chance, Level 16, No. 1 O'Connell Street,
Sydney, NSW 2000, Australia

www.cliffordchance.com