Privacy in Digital Media and Digital Advertising

IAB Australia *Industry Briefing: Privacy Update & the GDPR* event
Wednesday, 11 April 2018

Keynote address by acting ***Australian Information Commissioner and acting Privacy Commissioner, Angelene Falk****, at the* ***Interactive Advertising Bureau (IAB) Australia Industry Briefing: Privacy Update & the GDPR*** *event*

Good morning everyone.

I would like to acknowledge the Gadigal people of the Eora Nation as the traditional custodians of the land on which we meet today and pay my respects to Elders past, present, and future.

Thank you for the welcome and invitation to be here, and I commend the efforts of the IAB to make privacy the focus of the seminar.

My focus today is on how you can meet the privacy expectations of both consumers and regulators — a very timely topic given recent events.

The Facebook/Cambridge Analytica story has been in the headlines for a number of weeks, and has brought the issue of corporate responsibility, as it relates to privacy protection, to the fore.

Facebook CEO Mark Zuckerberg, has been quoted as saying, 'we didn't have a broad enough view of what our responsibility is. That was a huge mistake…'

Regardless of whether or not breaches of Privacy law are found to have occurred or not, these events are an opportunity for all businesses to consider whether their handling of personal information is not only compliant, but aligns with community expectations.

And it is important that businesses takes this opportunity - to ensure the benefits of data innovation to the community and the economy can be realised. Businesses need to be trusted custodians of the personal information of Australians. This is not only a legal imperative and a business imperative; there is a compelling case for businesses entrusted with the personal information of Australians to be ethical stewards of that information.

There have also been a number of developments in both domestic and international privacy regulation, which have brought the issue of privacy into sharp focus. These developments increase transparency, choice, control, and accountability.

So, I am going to start with an overview of the domestic and international privacy regulatory environment, before turning to the principles underlying consumer privacy expectations and the requirements of the Australian Privacy Act in more detail. Importantly, I will point to practical resources and tools from the OAIC to assist you in meeting those requirements.

Let us start with security of personal information; fundamental to trust in the digital economy. On 22 February 2018, the Notifiable Data Breaches scheme came into force in Australia — formalising data breach notification and assessment obligations for the range of agencies and organisations with personal information security requirements under the Privacy Act.

This morning, the OAIC published the first quarterly report on the data breach notifications received by the office. We have received 63 notifications since the NDB scheme commenced — which, when compared to the 114 notifications we received on a voluntary basis in the last financial year, shows the NDB scheme is on track to significantly increase the number of notifications handled by the OAIC.

You can find the full quarterly report on the OAIC's website — here are some highlights:

- Of the data breaches the OAIC was notified of — 51 per cent were reportedly caused by human error. 44 per cent of breaches were reported to be the result of malicious or criminal attack and 3 per cent the result of a system fault.
- The top three sectors that notified the OAIC of eligible data breaches were:
    - health service providers (24 per cent)
    - legal, accounting and management services (16 per cent), and
    - finance (13 per cent).
- 59 per cent of data breach notifications reported that the personal information of between one and nine individuals was affected. 90 per cent related to breaches involving the personal information of less than 1,000 individuals. Of the remaining 10 per cent of eligible data breaches the OAIC was notified of — 5 per cent involved the personal information of between 1,000 to 9,999 individuals, and 5 per cent involved the personal information of between 10,000 and less than 100,000 individuals.

These notifications will support improved understanding of the trends in eligible data breaches across industries – and promote a proactive approach to addressing security risks.

Similar requirements to the NDB scheme can be found in jurisdictions across the Asia Pacific, in the United Kingdom, and the United States. And, from the 25th of May, Europe will have harmonised data breach notification requirements with the commencement of the General Data Protection Regulation (GDOR).

The GDPR provides significant focus on privacy governance at an international level, with the requirements extending to businesses that have an establishment in the EU, offer goods and services in the EU, or monitor the behaviour of individuals in the EU. It introduces a number of new requirements for the EU, many of which are already reflected in Australian privacy law. At a high level, some of the key similarities are:

- Both laws foster transparent information handling practices and business accountability, to give individuals confidence that their privacy is being protected.
- Both laws require businesses to implement measures that ensure compliance with a set of privacy principles, and both take a privacy by design approach to compliance.
- Data breach notification is required in certain circumstances under the GDPR and under the Privacy Act.
- Privacy impact assessments, mandated in certain circumstances under the GDPR, are expected in similar circumstances in Australia.
- Both laws are technology neutral, which will preserve their relevance and applicability in a context of continually changing and emerging technologies.

Complementing the GDPR, the proposed Regulation on Privacy and Electronic Communications (e-Privacy Regulation) will update and repeal the existing e-Privacy Directive, to increase the protection of people's private life with a focus on electronic communications.

The proposed e-Privacy Regulation would expand the existing e-Privacy Directive remit from telecommunications providers to all electronic communications providers and includes updated rules for electronic marketing, and cookies.

Further, in Australia we will see changes in the data governance environment more broadly with the implementation of the new Consumer Data Right, which will be first rolled out in the financial sector. This new right was central to the Productivity Commission's data reform proposals arising from the *Data Availability and Use* inquiry in 2017 — which sought to enhance data mobility in order to derive the economic benefits of increased competition across industries.

The Consumer Data Right will give customers a right to direct that their data be shared with others they trust, so that they can benefit from its value.

The Australian Competition and Consumer Commission will promote competition and customer focussed outcomes through the Consumer Data Right— and the OAIC will work to ensure that strong privacy protections are fundamental in the design and implementation of the Consumer Data Right as it is applied across industry sectors.

While these changes are substantial in various ways —in reality the recent developments in privacy regulation are responding to enduring community concerns and a broad objective to ensure individuals and the community benefit from increasing data capabilities while having personal information respected and protected.

In our long-running national community attitudes to privacy surveys, we have consistently found that about three in five Australians have avoided a business due to privacy concerns.

In our 2017 survey, 69 per cent of Australians said that they were more concerned about their online privacy than they were five years ago.

And especially significant, is that when it comes to the secondary use of personal information, such as where one organisation purchases customers' data off another for direct marketing — 86 per cent of people perceived this as a *misuse* of personal information.

And we can all recall various instances in recent years where organisation's trustworthiness has been publicly scrutinised as a result of perceived privacy risks, or the failure to act promptly in response to privacy risks.

When consumer trust is lacking it hinders an organisation's ability to develop a social licence for innovative uses of data, and undercuts efforts to improve data mobility and analysis — two key ingredients to realising the potential benefits of data.

In today's environment, where data is effectively the lifeblood of various business operations, privacy must be integrated throughout an organisation.

Fostering a privacy culture, which extends from the collection of personal information to its eventual deletion, can ensure you are poised to identify and quickly respond to privacy risks.

So, how do you go about supporting an effective privacy culture in today's data-driven world?

The Privacy Act specifies that the personal information collected by businesses must be reasonably necessary for its functions and activities. For collecting sensitive information, (eg health, racial origin, political opinions) generally there is an additional requirement for consent.

Collection must also be by lawful and fair means. So these are the foundational principles that must be considered.

The Privacy Act is also about ensuring transparency and accountability.

Transparency enables individuals to make informed choices about sharing their personal information and to exercise control.

Transparency also ensures organisations are accountable for personal information protection – and for when things go wrong.

The Notifiable Data Breaches scheme formalises a long-held community expectation along these lines.

In our 2017 Australian Community Attitudes to Privacy Survey, 94 per cent of people said they should be told if a business loses their personal information.

Notifying individuals when they are at a likely risk of serious harm provides individuals with the chance to take steps to protect themselves.

And importantly, the NDB scheme reinforces that businesses have a responsibility to their customers – not only to protect personal information, but to be clear about what happens to the personal information they are entrusted with.

When understood in this way, it becomes clear why a business can face significant public backlash if it appears to have concealed, or attempted to conceal, a data breach — while on the other hand, prompt notification can reduce the reputational impact of a breach by demonstrating that an organisations takes their role as a data custodian seriously.

Understanding privacy as being about transparency and accountability also clarifies the apparent disjuncture between Australians voicing concerns about their privacy, and their willingness to share personal information with various organisations online.

The view that personal information is *traded* with an organisation, and that the individual cedes any say in how that information should be handled, does not align with community expectations and the protections of the Australian Privacy Act.

So, the question each business and agency must ask is: how do the principles of transparency and accountability operate in practice and how can we best meet them?

One essential and enduring consideration is how you communicate with your customers about privacy. The hallmark of the Privacy Act is transparency — and as part of this, you must have a clearly expressed and up-to-date privacy policy and privacy notices.

Your privacy notices should be a communications tool, not a litigation tool. It is an opportunity to explain how you handle personal information to consumers in a way that is easy to understand and is fair.

Many businesses can do better on this front. People need clarity on your personal information handling practices, and this needs to be presented in innovative ways; point in time / transaction specific notices, layered information highlighting the most important privacy matters, linking to your full privacy policy that is easy to find. The language you use needs to be simple — you could also consider incorporating visuals.

This will also support your compliance with obligations to attain customer's consent and help ensure you are collecting personal information fairly.

Consent in privacy matters has gained renewed attention with the GDPR — which expands on the previous definition of consent in the European Data Protection Directive to include the requirement that an individual's consent be an unambiguous indication of their wishes, and provided by a statement or by a clear affirmative action.

Consent is relevant to a number of the Australian Privacy Principles, namely those dealing with the collection of sensitive information (APP 3), use and disclosure (APP 6), direct marketing (APP 7) and cross-border disclosure of personal information (APP 8).

Under APP 6, for example, a regulated organisation must not use or disclose personal information for a purpose other than the primary purpose of collection, unless the individual consents to this secondary use or disclosure, or another exception applies.

I'll also briefly highlight APP 7 – which relates to direct marketing.

Under APP 7, consent is needed for direct marketing that uses or discloses sensitive information, such as political opinions or religious beliefs.

Personal information other than sensitive information may only be used for direct marketing if other requirements are met.

Both APP 7.2 and APP 7.3, for example, require you to provide a simple way for individuals to request not to receive direct marketing communications – or 'opt-out'.

This again highlights how central transparency and clear communication is to privacy compliance.

But of course, transparency about privacy must also be backed up by robust governance that effectively minimises privacy risks. Privacy must be a high order priority for your organisation, with senior engagement and accountability.

We have a range of guidance available on our website that can support you in this — but I would like to draw your attention specifically to our recently published *Guide to Data Analytics and the Australian Privacy Principles*.

Data analytics is increasingly prevalent across organisations, and it is highly valuable in understanding and meeting consumer needs.

But it also presents unique privacy challenges — including the potential to generate new information via inference. Data analytics has the potential to reveal more information about someone than they choose to share — including, for example, their state of mind, or their philosophical or political beliefs.

The *Guide to Data Analytics and the Australian Privacy Principles* highlights strategies to manage potential privacy risks in this regard.

This central strategy is embedding privacy by design. A requirement of the Privacy Act and the GDPR.

This term, 'privacy by design', describes a holistic approach where privacy is integrated and embedded in an organisation's culture, practices and processes, systems and initiatives, from the design stage onwards.

A central component of achieving this with any project involving personal information is conducting Privacy Impact Assessments, or PIAs.

A PIA is a practical tool, which assists organisations to identify and address privacy risks early, rather than attempting to 'bolt-on' solutions when the risk materialises.

Specifically, a PIA:

- systematically assesses the privacy impacts of a project, and
- recommends strategies to manage, minimise, or eliminate those impacts entirely.

Secondly, it is important to consider whether or not personal information is required for any particular activity. In some circumstances, de-identified information may be sufficient.

De-identification involves the removal or alteration of information that could reasonably identify a person.

In addition to removing direct identifiers such as names and addresses, de-identification requires considering whether any particularly unique personal information should be obfuscated, and any controls you might put in place to reduce the risk of re-identification. For example, you may put in controls around who is able to access a data set.

It is not always possible to draw a bright line between personal and de-identified information. De-identified information may, in particular contexts, become re-identifiable. For that reason, de-identification is an exercise in risk management rather than an exact science.

For data to be considered 'de-identified', the risk of re-identification in the context it is released must be very low – with no reasonable likelihood of re-identification occurring.

For further guidance on this, you can read the *De-identification Decision Making Framework*, a joint publication between the CSIRO's Data61 and the OAIC, which provides operational advice on de-identification. The OAIC also has guidance on our website titled *De-identification and the Privacy Act*, together with guidance and eLearning on conducting Privacy Impact Assessments.

I have no doubt other effective privacy management strategies will be discussed further in the sessions that follow.

In conclusion, it is essential to be proactive in embedding privacy in your organisation and business practices through taking a privacy by design approach. This enables you to meet community expectations, and to build trust in your data management — trust which supports you in realising the benefits of data and meets your corporate social responsibilities.

Thank you – I am happy to take questions.

Please note this version may slightly vary from the version presented on the day.