benchtv
a benchmark production

# Précis Paper

## Changes to Privacy Law – Part 2

A discussion of the changes to Privacy Law both in Australia and around the world, and what this means for organisations in Australia.

**Discussion Includes**

- Tips for lawyers interacting with IT Professions
- Preparation for the General Data Protection Regulation (GDPR)
- Identification

# Précis Paper

## Changes to Privacy Law – Part 2

In this edition of BenchTV, Anna Johnston (Director – Salinger Privacy, Sydney) and Stephen Wilson (Director – Lockstep Consulting, Sydney) provide insight into how Australian organisations may best prepare for the changes to privacy law both in Australia with the introduction of the Data Breach Notification scheme, and overseas with the General Data Protection Regulation (GDPR) in Europe.

Tips for lawyers interacting with IT Professions

1. Challenges arise for those of a non-legal background when dealing with privacy obligations. This can be aided by those with a comprehensive legal understanding of privacy obligations by being aware of the language that they are using.

2. If lawyers can orientate engineers to think about personal information in terms of how information is flowing, where it is being aggregated, whether it is needed, and so on, all parties are able to properly engage.

3. There is also a challenge in people understanding the breadth and scope of personal information, as many people believe personal information to only be details such as their name, address, bank account details and so on, even though personal information covers all information that may identify, or reasonably identify, a person.

4. It is also important to note that privacy obligations are not just limited to unauthorised disclosure. The privacy principles provide for much broader circumstances than just a breach of confidence. Privacy obligations cover the entire life cycle of how personal information is handled, from collection through to disposal.

5. The General Data Protection Regulation (GDPR), to be introduced in Europe in May 2018, may be the first taste of serious standards and norms that are needed to produce an orderly data economy. If data is so economically important, than the GDPR may be the first of what will probably be a wave of reforms that will give the data economy some order and predictability.

Preparation for the GDPR

6. Both the GDPR and the Australian Privacy Act (*Privacy Act 1988* (Cth)) have an accountability principle which provides that organisations need to adopt tools, systems, methodologies, and so on to say that they are proactively managing their compliance with the other privacy principles.

7. A Privacy Impact Assessment (PIA) is one of those methodologies. As a result of some of the more embarrassing privacy fails of the Federal government, from July 2018 Privacy Impact Assessments will become mandatory for all Australian government departments when they are designing what is considered to be a high risk project. The new Australian government Privacy Code starts on 1 July 2018.

8. Privacy Impact Assessments aim to be proactive about identifying privacy risks in the early stages of project design. At the design stage it is necessary to consider what the community and stakeholder expectations are, particularly about how the customer/citizen/patient's information should be collected, used and disclosed.

9. Privacy Impact Assessments deliberately aim to look beyond strict legal compliance, and actually think about what is needed for organisation to do right by their customers and meet their expectations.

10. Privacy Impact Assessments are sometimes compared to an audit, but a PIA is more in the design stage of a new project, compared to an audit which can be seen as a review of something that is already in place.

11. It is necessary to make sure that not just the design of the system itself will be the most privacy protective that it can be, but that the management of that project will also consider all of the privacy risks and how best to handle them.

12. When conducting a PIA the organisation should be looking for the foresight that has been exhibited in the way the system is put together. What will be the ongoing accountability, will the staff, or have the staff already been trained in what their responsibilities are? If you get a privacy complaint does everyone know what is supposed to happen and how it is to be handled, and so on.

13. The design of the data collection system itself is also important – does it only collect necessary information, does it only allow use of that information for defined and appropriate purposes, etc.

14. Consent is another factor that must be remembered. If an organisation wants to gather data for a purpose, it is not difficult to set out their stance in order to obtain consent, it just must be clear and obvious to the individual.

<u>Identification</u>

15. If an organisations believes that their data is outside the scope of the *Privacy Act 1988* (Cth) because they have de-identified the data, they run the risk that another company could put the data together with their data and potentially discover personal information.

16. There is no simple guide to de-identification of data. One of the problems is the misunderstandings about the language used as in some sectors to de-identify means something quite specific – it means to strip out direct identifiers, but it can have other meanings in different contexts.

17. The *Health Insurance and Portability and Privacy Act* (HIPPA) in the United States, for example, talks about how to handle patient records. It essentially provides that if the organisation de-identifies the information, then privacy obligations do not apply. It works on the presumption that if one cannot identify a record, then no privacy harm can be done.

18. In the HIPPA, de-identify means to strip out a particular 18 fields which are set out in the Act. The problem with that kind of approach to legislation is that the second you write down a list of 16 fields, it can become out of date, for example fax numbers. Also, while these particular categories may apply in one context, this does not mean the categories can be put across all other contexts.

19. Even in the context that the HIPPA applies, it creates a standard for de-identification but it is not a promise that the end result is non-identifiable forever, or for any context.

20. An example of the problems of de-identification is evidenced in Australia by the Federal Department of Health. The Department of Federal Health took 30 years of MBS and PBS data, cut a 10% slice of the whole data set and de-identified it, and published the information online for use in public interest research purposes.

21. The problem they then found was that the computer science faculty at the University of Melbourne found that the de-identification protocols that had been applied were not strong enough. It was possible to re-identify some of the doctors involved through their Medicare ID – and once it was possible to identify the doctor, there was potential to start to identify patients and so on.

22. There are a couple of different reasons why de-identification might not work to remove the risk of being able to identify someone:

    1. If the method of de-identification itself is fallible – for example the encryption used in the MBS/PBS data set could be decrypted/reversed.

2. Even if you have stripped out all of the identifiers, the name, date of birth, unique I.D, and so on, the attribute data may be uniquely identifiable.

23. There is a middle ground that must be met in terms of preserving people's privacy, while also being able to provide valuable information for social/medical research. Ideally, there must be some kind of secure system in which the data is held in order to navigate public health outcomes vs individual rights. It is suggested that researchers should need to apply to get access to the data, and they should only be able to access under certain conditions. This is a safer approach than the wholesale release of data.

24. In both the public sector and private sector, we are beginning to see that the idea of having completely free information is a bit simple. We have underestimated the risks of open data and open government. It is likely we will see a big cultural shift in the understanding of what the privacy risks are of big data, and big data analytics. Privacy laws are there to protect individual's physical safety, human dignity and integrity.

25. It is important to remember those rights, as well as the need to innovate and use data analytics for public interest purposes such as medical research.

<u>Key Takeaways</u>

26. The new data breach notification laws and the GDPR may seem scary, but it is also manageable. A lot of the privacy laws and principles under those laws are based on common sense and good manners.

27. If an organisation treats customers with respect, and treats their personal data with respect by working their way through the privacy principles it gives organisations a good road map for what is expected. There is guidance available from regulators and consultants, helping organisations with a step by step approach to complying with the relevant laws and principles.

28. At an immediate level, for an Australian organisation or a lawyer advising a company covered by the Australian principles or the GDPR, there are basic things you need to ensure you have covered:
    1) Understand if and when you are regulated by Australian and/or European privacy law
    2) Make sure your privacy policy is up to date and reflects both the Australian laws and the GDPR. There are some specific detailed requirements set out in the GDPR.
    3) Think about if you are processing, using or disclosing information on the basis of consent that your consent is very robust.

4) Make sure to take a proactive approach to privacy risk management, for example ensure that staff are trained, Organisations should consider using privacy impact assessments and so on.
5) Make sure there is a data breach response plan for when things do go wrong.

## BIOGRAPHY

Anna Johnston

Director – Salinger Privacy, Sydney

Anna Johnston is one of Australia's most respected experts in privacy law and practice. After serving as Deputy Privacy Commissioner for NSW, Anna founded Salinger Privacy in 2004 to offer specialist privacy consulting services. Salinger Privacy provides advice on managing privacy risks to clients including tech start-ups, Established businesses and government agencies. Salinger Privacy also offers a suite of privacy compliance tools including template policies and procedures, checklists, and eBooks including Demystifying De-identification and the Privacy Officer's Handbook. Anna holds a first class honours degree in Law and was admitted as a Solicitor of the Supreme Court of NSW in 1996, but no longer practices as a solicitor.

Stephen Wilson

Director – Lockstep Consulting, Sydney

Stephen Wilson is a leading researcher, analyst and innovator in privacy and security, and one of the world's most original thinkers in digital identity. His privacy expertise comes out of highly creative research into the complex interplay of privacy and security, and is based on many years work in the sensitive sectors of healthcare and government. He has developed and patented unique Privacy Enhancing Technologies for mobiles and IoT, and pioneered new privacy engineering techniques. Furthermore, Stephen is a past member of the Australian Law Reform Commission's privacy reform technologies subcommittee.

## BIBLIOGRAPHY

Legislation

*Privacy Act 1988* (Cth)

*General Data Protection Regulation (GDPR)* (EU) 2016/679

*Health Insurance Portability and Accountability Act of 1996* (HIPAA; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996)