ISSUE #79 JULY / AUGUST

PRESIDENT’S FOREWORD ................................................................................................................................................................................... 3
OAIC AUGUST UPDATE – PREPARING FOR THE INTRODUCTION OF MANDATORY DATA BREACH NOTIFICATIONS ............................................. 4
PRIVACY, INFORMATION SHARING AND TRUST IN THE HEALTH SECTOR, OH MY! .......................................................................................... 5
THE EU GENERAL DATA PROTECTION REGULATION AND ITS IMPACT ON AUSTRALIAN AND NEW ZEALAND COMPANIES ............................. 8
PRIVACY PROTECTIVE FRAMEWORKS AND METHODOLOGIES FOR DATA SHARING PROJECTS ................................................................. 12
AIR NEW ZEALAND LAUNCHES PRIVACY INITIATIVES ....................................................................................................................................... 15
HEALTH DATA GOVERNANCE: RE-IDENTIFICATION OF HEALTH RECORDS ........................................................................................................ 16
DON JUAN AND PROTECTING REPUTATIONS IN AN OPEN DATA ECONOMY .............................................................................................. 20
EVENT CALENDAR - METADATA & THE PRODUCTIVITY COMMISSION REPORT - PANEL DISCUSSION.......................................................... 23
EVENT CALENDAR - PRIVACY AFTER HOURS  .................................................................................................................................................... 24
EVENT CALENDAR - iappANZ 2017 SUMMIT ................................................................................................................................................... 24
JOB OPPORTUNITIES ......................................................................................................................................................................................... 24

Privacy Unbound is the journal of the International Association of Privacy Professionals, Australia-New Zealand (iappANZ), If you have content that you would like to submit for publication, please email: journal@iappANZ.org

The Journal Advisory Committee is comprised of the following iappANZ board members and members:

- Carolyn Lidgerwood
- Katherine Gibson
- Veronica Scott
- Kyle Lees
- Marta Ganko
- Emma Kulinitsch

Please note that the content published in the Journal should not be taken as legal or any other professional advice.
This edition of Privacy Unbound is the perfect follow up to the recent Data + Privacy Asia Pacific Conference hosted by the Office of the Australian Information Commissioner. It includes articles on several of the topics that were discussed, for example the impact of the EU General Data Protection Regulation on Australian and New Zealand business and the ever-evolving discussion around de-identification, especially in healthcare.

Directly after concluding the highly engaging and successful Data + Privacy Asia Pacific Conference we hosted a Privacy after Hours event in Sydney. This was the best attended iappANZ social event I think I have ever been to (outside of the post Summit drinks). It was just brilliant to have an opportunity to catch up with so many of you who had made it to the event. I have it on good authority that iappANZ members were still chatting away at closing time.

Looking ahead we have a series of awesome panel sessions coming up across Australia as a follow up to our previous events about metadata and the Productively Commission report. We also have several Privacy after Hours coming up. Check out the back few pages for all the details. There you will also see all the information for the highlight of the iappANZ calendar, the annual Summit which this year is has the theme ‘Walking the line: Privacy & Personalisation’ and will be held in Sydney on October 3rd. The Summit Advisory Committee led by Board Director, Melanie Marks has been working extremely hard to make sure that this year’s conference is the best ever. Tickets are selling quick so be sure to get yours while we still have the early bird offer in play until Wednesday, 16 August. You can register [HERE](#).

Our search for the best CEO we can possibly find to help deliver the iappANZ strategic plan continues. We are still accepting applications and details are [HERE](#).

In a few weeks’ time, the 2017 Board will be meeting for the last time in person before the Summit and the Annual General Meeting. At the AGM which will directly follow the Summit we will also holding the election for 2018 Board Directors and Executive Officers.

We very much encourage all our members to consider whether they would like to stand for a role on the Board. Details about how to do that will be sent out in September. I personally have thoroughly enjoyed my time on the Board both as a Director and for the last two years, as President. I strongly believe we need to balance experience with new ideas and leadership and as such will be standing down as President in October. I do, however, very much hope to remain on the Board to assist the new President and Executive with anything they need to continue to drive the initiatives that support our strategic plan.
Throughout 2017, the OAIC has been working with the business community to ensure they understand their obligations under Australia’s mandatory Notifiable Data Breaches (NDB) scheme, which commences on 22 February next year.

For many businesses and agencies, the information provided on the OAIC’s NDB webpage will be familiar — in fact, many will already be well prepared for the NDB scheme. This is because the NDB scheme formalises a longstanding community expectation — transparency in the management of personal information.

Clearly communicating privacy management practices is essential to gaining, and keeping, consumer trust. As revealed by the 2017 Australian Community Attitudes to Privacy Survey — 58 per cent of Australians have avoided a business because they had privacy concerns — a figure which has been consistent with the OAIC’s previous community surveys.

The expectation for transparency extends to when things go wrong — and a data breach occurs. Ninety-four per cent of people said they should be told if their information is lost by a business, and 95 per cent echoed this belief in relation to government agencies.

This shows an all but unanimous endorsement that the NDB scheme is already a consumer expectation. In notifying individuals of data breaches that may negatively affect them, organisations demonstrate that customer privacy rights are taken seriously. It is therefore unsurprising that over time, the OAIC has increasingly received voluntary data breach notifications.

Mandatory data breach reporting also brings Australian businesses in line with what is increasingly an international standard — with similar developments to the NDB scheme in the European Union, and jurisdictions in North America and the Asia Pacific. Australian organisations operate in a global regulatory system — and to ensure that compliance is simple, and regulators can coordinate their efforts more readily, it is essential to engage both international privacy authorities and businesses in discussions on privacy governance.

For further information about the NDB scheme visit www.oaic.gov.au/ndb.
PRIVACY, INFORMATION SHARING AND TRUST IN THE HEALTH SECTOR, OH MY!

Samantha Fitch
PhD Student, School of Population Health, University of Auckland

Samantha Fitch PhD shares with us her findings from two empirical studies she carried out in New Zealand. In summary, patients expect their General Practice Doctor (“GP”) to keep their health information confidential and only share the information as necessary or where appropriate - an outcome which has its foundations in the trust a patient has in their GP. Trust is an important factor which is likely to influence consumers’ expectations on how their personal information is handled in many other sectors and Samantha invites us all to consider trust in the role of privacy.

Exchanging high-quality information is vital in many sectors, and in health it is crucial for a health system focused of achieving better health outcomes, access to services, and delivering relevant clinical information to inform decision making. Health information is collected in the context of health professional/patient relationships that are (or should be) predicated on trust and confidentiality. While this claim may seem relatively uncontroversial, establishing the role of trust for individual’s attitudes and expectations of information sharing is more difficult.

Findings from two empirical studies outline patients’ expectations that GPs must ensure patient privacy and confidentiality, and should only share information as necessary or appropriate. While levels of trust in health professionals and organisations are high, patient knowledge and awareness of the rules and practices around information-sharing are low. Further these matters are not often discussed between GPs and patients, although patients do not appear to be concerned by this. Patients showed little concern about information being shared within the health system or with health professionals, but had concerns about the potential implications of third-party sharing. While some actions may disrupt or breach trust there are ways that GPs can seek to rebuild trust with patients. The findings confirm the importance of trust for the GP–patient relationship and suggests that patients’ trust GPs to use and share information when necessary and for their benefit.

These findings highlight four interesting points:

1. Trust in health professionals and organisations in New Zealand is high. In general, trust in professionals (like Nurses and GPs) was higher than that of health organisations. This may be attributed to the level of experience of an individual with particular professions as opposed to health organisations. In this context, the face of the profession or organisation (i.e. the person you interact with and build an expectation of trust in relation to) and particular interpersonal relationships have an impact on levels of generalised trust. However, while trust is high, knowledge and awareness about the practices and rules around information sharing are low. Trust in the GP allows patients to bridge the gap left by the unknowns. In doing so, patients trust that their GP will act appropriately and maintain confidentiality and privacy unless it is necessary to disclose to others.

2. Expectations of privacy vary from individual to individual. While one person might think their information should be shared with everyone, another may feel that their information should remain solely under their control. In conversations with patients, some thought all the information they had ever given health or social services was held in one location, accessible to all. Others lamented that more information was not shared between primary and secondary care (GPs and hospitals for example). While some ideally wanted to know each and every time their information was accessed or used. I use these illustrations to signify the variation in attitudes and expectations around privacy and information sharing.

3. There is some degree of concern about the type of information being shared and the recipient of that information. The more “sensitive” that people perceive information to be, the more reservations they have about sharing it. Conversely, information that is perceived as “boring” or “inconsequential” is more likely to be acceptable to share. In talking about different health professionals and the sector more generally, it was clear that sharing information with health professionals and even broader within the health sector was acceptable. However, there were more concerns about third party sharing, particularly if it was unclear what the purpose was. Sharing within the health sector aligned with patient expectations that information would be shared when necessary and appropriate in the delivery of care, or where there was some other benefit to the patient.

4. Trust is important within the doctor-patient relationship, and when it has been challenged or broken it may be ameliorated. Trust is multi-faceted but it comprises communication, a mutual relationship and caring as well as the competence, knowledge and skill of the doctor. Patients varied in
whether they thought trust could be repaired in a situation where it was challenged or broken (for instance with a data breach). For those who thought it was amenable, it would require an apology (or other form of communication), action to remedy the situation, and efforts to ensure it would not happen again. Furthermore, the extent to which trust and privacy breaches are amenable to repair or restoration depends on the extent to which expectations are oriented or reoriented through communication.

Overall, this research outlines the importance of trust in information sharing between patients and GPs. The centrality of relationships and communication within information sharing need to be respected as such. Information sharing is about more than mere exchange, and this is why trust is so important when we think about disclosures, information sharing and privacy. Not only trust in terms of the perceived or proven trustworthiness of the person receiving the information but also about the privacy, confidentiality and security of that information as it changes hands.

I encourage an ongoing thought about the role of trust in your current situation or privacy practice and welcome feedback and discussion around this issue.

ABOUT THE AUTHOR - SAMANTHA FINCH

Samantha completed a PhD looking at Trust as it relates to Information Sharing (particularly in the health system). This topic combines several of her passions - ethics, public policy, informatics, privacy and public health. She is based in Auckland and currently works as a policy analyst for the Ministry of Health.

For more information contact: Samantha_Fitch@moh.govt.nz or VISIT HERE
2017 Summit

Privacy & Personalisation

Walking the Line

Tuesday, 3 October 2017
Dockside, Cockle Bay Wharf, Sydney, NSW

Register at www.iappanz.org
THE EU GENERAL DATA PROTECTION REGULATION AND ITS IMPACT ON AUSTRALIAN AND NEW ZEALAND COMPANIES

Nicola Hermansson
Data Privacy Leader, EY Auckland

With all the noise about the EU General Data Protection Regulation (GDPR) most organisations can be forgiven for thinking the sky is falling. Don’t worry - it’s not.

Having recently moved to New Zealand from delivering privacy services in the UK, I have been in the middle of the GDPR whirlwind for the past few years, helping organisations break through the noise and understand the impact GDPR has on their organisation. Yet the same wave of urgency and concern doesn’t seem to have spread to this side of the world. Many organisations may even be thinking it’s an EU issue, nothing for them to worry about. But that’s not necessarily the case.

GDPR is an EU regulation, which will be enforced from 25 May 2018, and is designed to protect and empower individuals in the EU, giving them control over their personal information whilst imposing strict rules on organisations that collect and process this data, anywhere in the world.

If your organisation is located outside the EU, and offers goods or services to, or monitors the behaviour of, individuals in the EU, then GDPR applies to you.

Many organisations will be viewing GDPR as a tax, but those organisation that take privacy seriously and embrace the changes, can use GDPR to obtain a better understanding of their business, gain the trust of their customers, win more business and differentiate themselves from their competitors.

So let’s consider the key changes and some practical steps you can take. Ask yourself these questions:
• Does GDPR apply to your organisation?
• If so, how can you approach it in a rational way?
• If it doesn’t, how can you use GDPR as a baseline for privacy good practice, to add value to your organisation?

Key changes

GDPR brings with it some significant changes. However, most are good baseline privacy requirements that all organisations should consider implementing. Some of the key changes include:
• Accountability: GDPR increases the accountability of organisations entrusted with processing and managing personal information. Organisations will be required to demonstrate their compliance by documenting data and processing activities, completing Privacy Impact Assessments, and performing privacy audits and policy reviews. This may be a heavy burden for organisations that have not previously invested in privacy, but the investment can enable more effective data management and provide clarity on the data within an organisation. This can help organisations to identify ways of getting the best value from that data and ways of adding value to the services they provide to their customers.
• Right to erasure: Organisations will have to facilitate individuals’ right to erasure. This means that, where certain conditions are satisfied, on request organisations must be able to identify where an individual’s personal data is located and then ensure it is erased. This is no easy task, given the propagation of data across organisations, countries, and to third party data processors.
• Mandatory breach notifications: Data breaches that could result in a risk to privacy rights must be notified to supervisory authorities within 72 hours. In some cases, this must also be notified to the individuals impacted. This can increase individual trust and build goodwill, and will require new policies and processes to be implemented.
• Consent: More stringent consent requirements include: consent must be active – doing nothing (eg, pre-ticked boxes) is no longer allowed; separate consents are required for different processing activities – they cannot be bundled together; supply of services cannot be made contingent on an individual consenting to processing that is not necessary for the service being supplied; individuals must have the right to withdraw their consent, and they must be clearly informed of this. These requirements will increase transparency for individuals, as well as more clearly define an organisation’s responsibility and the purpose for which they need to collect and use data. This should help prevent organisations from drowning in data by collecting more than they need or can manage efficiently.
• Data Protection Officer: Most organisations will need to introduce a Data Protection Officer (DPO) whose primary objective will be to oversee and manage privacy in an organisation, ensure GDPR compliance, and liaise with authorities and individuals. They must report to the highest level of management.
• Fines: The big change, leading to much of the panic, is the increased fines. Organisations can be fined up to 4% of their global annual turnover, or \euro20 million, whichever is greater. These penalties apply not only to a data breach but to a wide range of infringements, including basic procedural contraventions.
What should I do?

There are some clear steps your organisation can take to determine if GDPR applies to you, to understand what you need to do and to take action in a sensible, controlled and practical way.

Step 1 - Does GDPR apply?

Use the questions in the box below to work out if GDPR applies to your organisation. If you determine that it doesn’t, I would encourage you to use this as an opportunity to think about how your organisation can use GDPR requirements to improve privacy, demonstrate you are putting your customers first and to add value to your business.

Step 2 - understand what personal information you have in your organisation.

This is really important. Without understanding what personal information you have, how much you have, how sensitive it is, where it is and what it is used for, it will be impossible to understand your privacy risks.

Step 3 - perform a risk assessment.

This is when you ask the questions:

- What can go wrong?
- How likely is it that it will go wrong?
- What is the impact to our organisation and to the individual affected if it does go wrong?
Step 4 – understand your risk tolerance.

If you have a high risk tolerance, you may be willing to accept some of the risks you identified. But if your risk tolerance is low, you may not be willing to accept many risks.

Step 5 – determine the controls you need.

The level of control you need to put in place will be informed by your risk assessment. For most organisations, the ‘gold standard’ will not be required.

Step 6 – develop your privacy improvement plan.

Work out the amount of effort, in terms of time, resources and budget required to deliver on your plan.

Phew … it doesn’t apply to me

If you are thinking ‘Phew… it doesn’t apply to my organisation’… don’t stop reading now. Organisations which fall through the cracks and are not bound to GDPR should not ignore the noise it has been creating.

The public is becoming increasingly concerned about the treatment of personal information. The NZ Privacy Commissioner’s Office 2016 Privacy Concerns and Sharing Data Survey1 shows approximately two-thirds (65 percent) of New Zealanders are concerned about privacy and most respondents (75–81 percent) were concerned about issues related to identity theft, credit card and banking details, businesses sharing personal information and security of information.

The Office of the Australian Privacy Commissioner Australian Attitudes to Privacy Survey2 tells us 69% of Australians are more concerned about online security than they were five years ago. Security concerns mean 58% decided not to deal with some businesses.

How organisations champion their right to privacy and manage data securely is fast becoming a market differentiator and a value-add that customers are demanding. With the increasing number of data breaches making the headlines, individuals are searching for organisations they can trust.

At its minimum, GDPR offers organisations a good baseline of privacy and data management controls that every organisation should adhere to. It establishes a set of standards and practises which, if implemented appropriately, should appease and prevent the public’s key privacy fears.

At the same time, it should mitigate damage caused by a data breach and give organisations greater control over data in their possession.

Top tips

Having worked on many privacy programmes, here are some of my top tips for delivering a successful programme.

1. **Get leadership buy in** – don’t be a lone ranger. If you do not get leadership support and accountability for the programme, this will become a painful journey with lots of bumps (and possible crashes!) along the way.

2. **The privacy programme should be owned by the business**. The DPO or privacy team should not ‘do’ this to the organisation. A privacy programme should be owned and driven by the business: privacy is a business issue which, if addressed effectively, can add value to an organisation.

3. **Understand the value of good privacy and sell it to the business**. To get business buy-in, privacy must be ‘sold’ as more than a compliance exercise. Understand the value of getting privacy right. It is a much more powerful and compelling message to senior leadership to say investing in privacy will win us more business and make our customers happy, rather than we need to do this to be compliant.

4. **For most organisation a privacy gold standard is not required**. Take a risk-based approach and design a solution that meets the needs of the business, is practical, achievable and will add value.

The time to act is now

The sky is not falling but that does not mean organisations should be complacent. The global privacy landscape is changing, not just in the EU but here in New Zealand and Australia too.

We are starting to see GDPR requirements seep into the laws here – the new mandatory breach notification rules in Australia and the proposal for $1 million fines, mandatory breach notification and the right to data portability in New Zealand. For New Zealand to maintain its EU adequacy status, New Zealand laws need to keep pace with the changes in the EU.

Organisations who are yet to fully understand the need to implement effective privacy and data management controls need to act now, as the countdown for the GDPR is on. Preparation is essential, but will require time and effort. The GDPR offers a minimum standard of controls which all organisations should observe. The benefits of compliance, whether required or not, are invaluable.

---

ABOUT THE AUTHOR – NICOLA HERMANNSON

Nicola is a Director at EY and leads the New Zealand Data Privacy practice. She has over 13 years’ experience delivering privacy, PCI DSS and information security services to clients across the public and private sector. Nicola is a dynamic leader who leads a team of privacy professionals, bringing an unique mix of industry, consultancy and legal experience to deliver exceptional data protection assurance and advisory services to her clients.
PRIVACY PROTECTIVE FRAMEWORKS AND METHODOLOGIES FOR DATA SHARING PROJECTS

Peter Leonard
Principal, Data Synergies

Data sharing projects typically require accommodation of concerns of a variety of stakeholders.

Concerns often include:

- that where personally identifying information is disclosed and used through data sharing, that the use is for a purpose of which affected individuals had notice,
- that the data user is able to verify that, where required (for example, in relation to health information), affected individuals have given informed consent to this disclosure and use,
- information security, including guarding against threats from internal unauthorised intrusion and external threats including malicious attacks (denial of service, hacking etc.) and cyber-espionage,
- keeping clarity as to who ‘owns’, maintains and is responsible for control of distribution of data (for example as to which core data sets may be transformed by cleansing, normalising, key coding, merged or other transformations or value adds, as to ownership and of subsequent use of transformational code, algorithms and inferences, insights, and reports derived from data analytics conducted on these data sets),
- maintaining trust of citizens that information about them will not be used by government agencies or business enterprises in ways that are privacy invasive, ‘spooky’, contrary to accepted societal norms from time to time, or in ways that may lead to them suffering unfair adverse consequences,
- complying with restrictions in contracts and in statutes, and
- protecting confidential information and trade secrets.

Many data sharing projects fail to proceed due to an inadequate framework to resolve privacy concerns.

To date privacy concerns around data sharing have often been addressed by using ‘masking’ of identifiers: that is, the removal of personal identifiers and the pseudonymisation of data sets using transactor keys or tokens. However, some privacy advocates assert that technological advances and multiplicity of data points make re-identification of individuals from pseudonymised data relatively straightforward. In response, there has been extensive work in recent years in developing privacy protective risk management methodologies in order to specify appropriate and legally enforceable requirements for data linkage of data about individuals. These methodologies may be employed to properly protect data sets such as card transaction records, geo-located movement traces and patient level epidemiological health data, that otherwise may be vulnerable under reidentification attack.

Privacy risk management turns on recognising a distinction between de-identification and anonymisation. The stages of removal or obfuscation of direct (name) or indirect (mobile number, movement trace, email address) identifiers of any individual included in a stream of transaction data can be seen as steps along a continuum of de-identification. Effective anonymisation of transaction level information is the logical end point of that continuum. Anonymisation means the data transaction information still addresses a unique and distinct transactor, but does not enable the individual that is the unique transactor to be identified, whether from the information itself or from any combination of data points reasonably available to any entity that has access to the data stream or its derivations.

Of course, de-identification to the point of anonymisation can often be achieved by aggregation of individual data points, typically for the purpose of making comparisons or identifying patterns: that is, to show general trends or values without leaving granular indirect identifiers that might leave an individual identifiable within the data. Applying k-anonymity or like methodologies, values determined to be of ‘small numbers’ may be suppressed to minimise risk of reidentification, either through blurring or through omission altogether. Sometimes it is possible to de-identify data to the point where the transformed data is safe for public release because there is no more than a remote risk of individuals being identified: in this case, the data has been effectively anonymised. Of course, once the data is released the full artillery of re-identification techniques may be employed on the data by anyone, so anonymisation must be particularly robust, including over time.

Unfortunately, the utility of effectively anonymised data for many purposes, and particularly for epidemiological applications, is severely compromised by aggregation, suppression or blurring. In such cases, alternative measures must be taken that retain the usefulness of unique individualised data whilst still protecting the privacy of the individuals concerned. Clearly useful individual level data cannot be released publicly, but re-identification risk associated with its use may be managed through pseudonymisation combined with controls as to access and application of that data. This may be referred to as controlled (or safeguarded) release, only for use in a recognised ‘de-identification zone’. In the scenario of controlled release, the assessed harms from re-identification may be allowed to be higher than for data released into the wild. Assessed risk is a measure of the extent of threat by a potential circumstance or event and so typically a function of both the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence. Therefore, controls deployed in the safeguarded data environment may substantially reduce likelihood of attempts at re-identification while in that environment. Physical, system, human and permitted output controls as the perimeter of the safeguarded de-identification zone may ensure that outputs from that environment are appropriately aggregated or otherwise privacy protected. Thus, assessed harms from improper release of particular data sets from the safeguarded data environment may be high, but the risk that those harms will be suffered may be so effectively mitigated that assessed re-identification risk is remote.

In summary, data sets and data streams that would usually be considered too high risk to individual privacy protection may be managed within a properly planned, documented and implemented privacy management framework that can reduce re-identification risk to the point where this risk is remote within the particular context of controlled release and use. A similar risk assessment methodology may be applied to both controlled access and public release data sets, to determine the point at which re-identification risk is sufficiently remote for the particular context of use.
Two important consequences follow from assessment of risk requiring both assessment of harms and likelihood of those harms being suffered. First, where data is de-identified for limited disclosure or access, provided that disclosure or access has been appropriately, reliably and verifiably limited and controlled, re-identification risk will be significantly less than if that same data was put into the wild. Second, likelihood of occurrence might be mathematically expressed using an objective scale. But because harms are likely to be quite specific to the circumstance and particular individuals, a fact specific, contextual analysis is required. In any event, there is no regulatory clarity as to how a ‘low’ or ‘remote’ point of likelihood of occurrence is to be objectively and statistically measured, so assessment of risk has an inherently subjective element. That is why privacy impact analysis remains an inexact science, or as some information security experts see it, something of a black art. In any event, a privacy impact assessment should be conducted in relation to any project involving use of purportedly de-identified data which carries any reasonably ascertainable risk of re-identification of any affected individuals, both as to risks within the safeguarded data environment and as to outputs from that zone which themselves might be personally identifying. within the risk should have.

We have already noted that perimeter controls around a controlled environment may ensure that released outputs from that environment are appropriately aggregated or otherwise privacy protected. This aspect of safeguards requires particular attention in order to ensure that permitted inferences, insights and reports derived from data analytics conducted on the safeguarded data sets do not leave any individual reasonably identifiable and otherwise protect the underlying data in accordance with expectations and requirements of the contributor data custodians. This is an area where contractual restrictions are particularly important, but so too is specification of processes and procedures to ensure that these restrictions are understood, followed and verifiably reliable.

Often data linkage projects are outsourced to third parties, to leverage their data science skills and methodologies and to create separation from a data custodian’s personally identifying data sets. Data analytics services providers may in controlled environments facilitate privacy protective data linkage of individual level data. Relevant controls vary, but privacy and security by design compliant arrangements for data linkage of individual level data about individuals are typically based upon four key control elements:

- separation of persons or entities with access to personally identifying information from those persons or entities (‘trusted third parties’) conducting analytics using data sets which have been pseudonymised;
- replacement of direct or indirect personal identifiers in the merged data sets with a linkage code, or transactor key, which enables the service provider to infer that an identifiable transactor found in each data set is a unique transactor, although not identifiable;
- a combination of technical, operational, contractual and otherwise legally enforceable safeguards which reliably and verifiably ensure that uses of data outputs are only in accordance with stated purposes and that individuals that are the subject of transaction data are not re-identified and that records of personal information about those individuals held by any relevant party are not augmented or supplemented in any way through the controlled process,
- information governance oversight, data process controls, and change control processes and quality assurance processes that ensure that each of these things are reliably and verifiably implemented and then reliable in ongoing operation and that any change in data flows or deviation from required practices and procedures is promptly identified, considered and (if need be) addressed by appropriate risk mitigation measures.

Such arrangements are sometimes called ‘trusted third party arrangements’. However, the requirements that engender and enable ‘trust’ should be embodied in specific contractual obligations and associated work processes and procedures to ensure that the arrangements are appropriately privacy protective. These arrangements are accordingly not a matter of ‘trust’. The requirements are both legally enforceable and exacting to meet and to verify.

Of course, such exacting de-identification requirements are not required if affected individuals have given fully informed consent to particular data sharing. Consent is always the best solution, but often this solution is not available and use was outside the contemplation of the data custodians when consents were obtained and the relevant data collected. So often a view will need to be taken as to whether the act or practice of creating and using data linkage code is an act or practice of a data collector regulated by privacy law. Legal questions include whether pseudonymisation of personal identifiers itself an act or practice in relation to personal information which requires notice to or consent of the affected individual (and if so, how express that notice or consent needs to be), or is pseudonymisation an act or practice is akin to, say, anonymisation of personal information by aggregation up in reports and analyses? Further, to what extent can a party disclosing deidentified transaction level information and associated data linkage code rely upon that party’s assessment as to the likelihood of compliance of a downstream recipient with relevant prescribed safeguards? In other words, how active must the disclosing be in verifying that a downstream recipient will meet such commitments as the recipient is willing to give as to its compliance with the requirements which underpinned the disclosing’s decision to facilitate the data linkage? The answers to these questions in the Australian regulatory environment remain the subject of some debate and disagreement.

Conclusion

Data sharing of data sets between organisations is a young, but fast growing, area of data science practice. Trusted third party arrangements are a key aspect of controlled data sharing that address many of the privacy concerns that arise in relation to data release into the public domain. But maintenance of trust of consumers and citizens and other stakeholders as to (what they understand to be) “data sharing” depends upon businesses and governments building community understanding as to how appropriate settings as to privacy and security by design address legitimate concerns as to unconstrained data sharing. Citizens and their advocates should not be expected to rely upon assurances from governments and businesses as data collectors and sharers that they can be trusted to meet community expectations.

Requirements that engender and enable trust should be sufficiently transparent as to be understood by stakeholders. They should also be embodied in detailed contractual and legal obligations and associated work processes and procedures in order to ensure that the arrangements are appropriately privacy protective. The requirements are exacting, both to implement and to verify on an ongoing basis that the requirements are being
Privacy protective arrangements by design must ensure that processes and procedures anticipate and mitigate reasonably foreseeable risks of failures of processes through human error or oversight and other things that may go wrong.

The risks of failures of controls due to poor specification or monitoring are significant. The adverse consequences of failures may affect many projects beyond any particular project which suffers the failure: such is the interconnectedness of trust, and its loss, in an interconnected world. This is not an area for trial and error and iterative process improvements: it is important to get data sharing and data linkage projects right from the start. That said, we now have a developing international consensus around good practice in privacy risk management and risk responsive design in management of personal information and information security. Australia is well placed to be a leader in development of socially responsible data sharing and data linkage initiatives.

ABOUT THE AUTHOR – PETER LEONARD

Peter Leonard is a data, content and technology business consultant and lawyer and principal of Data Synergies, a new data commercialisation consultancy. Peter was a founding partner of Gilbert + Tobin. Following his retirement as a partner in 2017 he continues to assist Gilbert + Tobin as a consultant. He was voted by Sydney technology lawyers as ‘Sydney Information Technology Lawyer of the Year for 2016’ as awarded by Best Lawyers International. He is rated by Best Lawyers International 2017 as leading in the areas of Commercial Law, Information Technology Law, Privacy and Data Security Law and Telecommunications Law and Media and Entertainment Law.
AIR NEW ZEALAND LAUNCHES PRIVACY INITIATIVES

Jacqueline Peace  
Senior Manager Data Protection/CPO, Air New Zealand  
iappANZ Board Member

Air New Zealand marked Privacy Awareness Week with the launch of several initiatives driven by the Air New Zealand Global Privacy Office. We held an internal event at the Auckland Hub for Air New Zealand employees, with 160 attendees.

We were thrilled to have the New Zealand Privacy Commissioner John Edwards join us for the event, where he shared his views on how organisations like Air New Zealand can lead the way in privacy, and how changes to legislation overseas affects Air New Zealanders at an organisational and individual level. We recorded some key soundbites from John which were made available to employees via our internal internet. We also provided a podcast to enable employees to listen to the panel Q&A featuring the Privacy Commissioner, Chief Digital Officer Avi Golan, General Counsel & Company Secretary Karen Clayton and Senior Manager Data Protection / CPO Jacqueline Peace.

As an international airline, we handle personal information from our customers every day in order to provide a more personalised travel experience. Increased awareness about privacy ultimately affects the trust customers have in organisations like Air New Zealand, so we need to protect the personal information that is entrusted to us. Our programme initiatives were focussed on enabling every Air New Zealander to ‘think privacy & do the right thing’ at all times so that we do right by our customers and each other. Being informed about privacy is not only good for our business and our customers – we also focussed on the message that awareness is good for individuals in their daily lives – it helps when you can relate to it at a personal level. In our increasingly technology-focused world, and as the recent cyber-attacks around the globe have shown, personal information is becoming a more and more valuable commodity.

The launch of our new internal Global Privacy Office information hub pulls together a number of key resources for Air New Zealanders’ including information on new processes for handling privacy data breaches and what to do if a customer requests access to their personal information. New global training is available through our internal Learning Management System and we provided a refreshed Privacy Policy, Employee Privacy Statement and a new external facing Privacy Centre on our websites. This is the first in our evolution of the privacy statement to a more interactive and readable statement about how we handle personal information. We are working hard to take the message to our employees with frequent “stand-up” sessions to all our front of house employees. All the action, communications and new resources have created a buzz about privacy around the business. Whilst it was hard work, the “big bang” launch approach made an impact which we are super proud of.

ABOUT THE AUTHOR – JACQUELINE PEACE

Jacqueline leads the global privacy function for Air New Zealand and is based in Auckland. She has advised on privacy and data protection matters and implemented global privacy programmes for over ten years. Previous roles have included Head of Information Governance, GE Capital (covering the EMEA region) and independent privacy advisor for BP Ltd and Standard Chartered Bank, all based in in London. When she returned to New Zealand in 2014 she provided independent consulting services covering biometric and immigration related privacy matters and conducted high risk privacy impact assessments for government agencies.
HEALTH DATA GOVERNANCE: RE-IDENTIFICATION OF HEALTH RECORDS

Simon Lewis, Roland Fan, Sylvia Ng, Steph Baker
PwC

In brief

Australian governments have long recognised the potential of big data, which can provide the depth of insight about the community to enable genuine evidence-based policy development, public infrastructure planning, and service delivery innovation.

The intensive analysis of data sets drawn from a range of different sources to uncover important trends and insights, commonly referred to as ‘Big Data’, has a particularly important role to play in Australia’s health system, which comprises a complex web of medical, social and behavioural influences. Rich data sets exist at patient and system levels, reflecting the dominant role that Australian Governments play in our system, anchored in the Medicare Benefits Scheme (MBS) and the Pharmaceutical Benefits Scheme (PBS) and now-ubiquitous My Health Record (MHR).

Big data can improve population health, stimulate therapeutic innovation and enhance system efficiency and sustainability. The benefits can only be realised with the trust and confidence of citizens, bringing privacy issues into sharp relief. The use and management of data and health information is now regulated by the Privacy Act 1988 (Cth) (Privacy Act) and health records legislation in most States and Territories.

In this article, we consider some of the regulatory issues relating to the de-identification and re-identification of health records data, particularly in light of a September 2016 incident in which deidentified PBS / MBS data was re-identified. We also highlight the challenge facing legislators in managing the tension between protecting personal information and allowing innovation to enable the promise of big data to be realised.

Increasingly sophisticated data management techniques have been developed to de-identify health records information, to enable data to be used, whilst complying with regulatory obligations. Those same techniques may, however, enable data sets to be re-identified, highlighting the need for a range of responses to adequately protect personal information.

There is an inherent tension between using big data sets to benefit the community and the personal privacy of the individuals to whom the data relates. Appropriate policy, contractual and technical controls are needed to maximise privacy protections without limiting the usability of the information (by, for example, over-use algorithmic de-identification which can reduce the integrity of the information). Finding the right mix of controls will maintain public confidence and spur further innovation in the health sector, realising the potential of big data for better health outcomes and system sustainability.

In detail

Government 2.0 and the creation of data.gov.au

In August 2016, the Commonwealth Department of Prime Minister and Cabinet (PM&C) launched the much anticipated data.gov.au website with the intention of providing an easy way to find, access and reuse public data sets. Data.gov.au publishes a range of datasets from various government entities, including data sets relating to health, science, civic infrastructure, community services, finance management, and communications.

It is intended that data.gov.au will become a comprehensive repository for data from Commonwealth, State and Territory governments, and City Councils, although at this point it is predominantly data sets from several Commonwealth agencies. PM&C has recognised that expanding the data stack will be an ongoing process.

The creation of data.gov.au followed on from the Government’s ‘Declaration of Open Government’ (Declaration) and the declaration was a response to the ‘Government 2.0 Taskforce Report’. Through the Declaration, the Government committed to promoting greater participation in Australia’s democracy by acting as an open government “built on better access to and use of government held information, and sustained by innovative use of technology”. Data.gov.au facilitates the sharing of de-identified government information on a public platform.

De-identified PBS and MBS data sets were initially published, although following the re-identification incident, discussed below, that has now been removed. At this time the public disclosure of data relating to health and health care is relatively limited; there are twenty data sets available and a number of these are lists of sporting clubs and wellness providers, rather than therapeutic data sets.

De-identification of data

A common method of safeguarding collected personal information (particularly in big data sets) is deidentification. Personal information is ‘de-identified’ where it is no longer ‘about an identifiable individual or an individual who is reasonably identifiable’ under section 6(1) of the Privacy Act.

The ability to successfully de-identify information is an important enabler of big data, as it allows for large quantities of personal information and, in the case of health, highly sensitive personal information, to feasibly be sourced and prepared for analysis.

De-identification can be thought of as removing or modifying a person’s name, address or date of birth, although more sophisticated techniques exist; the Office of the Australian Information Commissioner (OAIC) has highlighted a number of these, including:

- removing or modifying quasi-identifiers (for example, significant dates, profession, income) that are unique to an individual, or in combination with other information are reasonably likely to identify an individual,
- combining information or data that is likely to enable identification of an individual into categories. For example, age may be combined and expressed in ranges (e.g. 25 – 35 years) rather than in single years (e.g. 27, 28 years of age),
- altering identifiable information in a small way such that the aggregate information or data is not significantly affected — a tolerable error — but the original values cannot be known

Privacy Unbound: Issue 79
with certainty, swapping identifying information for one
person with the information for another person with similar
characteristics to hide the uniqueness of some information,
• using algorithms to generate ‘synthetic’ data from original
data sources and substituted for it, while preserving some of
the patterns contained in the original data. This allows
systems to be tested with data that is realistic but poses less
risk of re-identification, and
• suppressing data, which involves not releasing particular
information that may enable reidentification, or deleting that
information from the dataset. Data suppression may impair
the utility of an information asset.

The challenge that the OAIC has raised in this respect is
understanding how organisations ensure deidentification is
‘correctly done’ (if, indeed, there is a ‘correct’ way to do so). The
appropriate deidentification method would depend upon the
sensitivity of the data, relevant organisational controls and the
analytical requirements, highlighting the need for an effective risk
assessment, often called a privacy impact assessment, to be
undertaken. The objective in undertaking the assessment should
be to ensure that personal data is appropriately protected whilst
retaining sufficient detail in the relevant data set to enable it to
be used for its intended purpose.

Overview of regulatory regime

The Privacy Act and the Australian Privacy Principles contained in
Schedule 1 of the Privacy Act (APPs), set out a regime for the
collection, holding, use and disclosure of data applicable to
Commonwealth agencies and organisations. The regime is based
on guiding principles rather than prescriptive requirements.
Importantly:
• when an agency or organisation collects personal data from
an individual, it must inform the individual of the purpose for
which it is collected so that the individual can provide
consent to its use and disclosure for that purpose. If the
organisation wishes to obtain consent for a secondary
purpose at the time of collection, it must state a specific
secondary purpose – a broad, ‘catch-all’ purpose will be
insufficient;
• the agency or organisation must not use or disclose the
personal data other than for the consented purposes unless
an exception under the Privacy Act applies. One exception is
the existence of a ‘permitted health situation’, which
includes where the use or disclosure is necessary for
research relevant to public health and safety and occurs
within relevant guidelines, and obtaining consent is
impractical, and
• where the agency or organisation no longer requires the
personal data for the purposes that it was collected, it must
destroy the data or take reasonable steps to de-identify the
data.

The opportunities presented by big data sets, including health
data sets, has led to a preference for deidentifying rather than
destroying data. If de-identified sufficiently, this means that
organisations may still be able to use, share, and publish such
information whilst preserving the privacy of individuals. As noted,
the method of de-identification which is ‘reasonable’ in the
circumstances depends on factors such as the type and sensitivity
of the data, and whether the data is qualitative or quantitative.
The matters for consideration of what is ‘reasonable’ in the
circumstances include:
• the amount and sensitivity of the information,
• the nature of the organization (including size, resources and
business model),
• possible adverse consequences to the individual if personal
information is not destroyed or deidentified,
• the organisation’s information handling practices (including
whether it outsources or transfers information to third
parties or overseas), and
• the practicability (such as time and cost).

Under the Privacy Act, the OAIC can also approve for the
purposes of the APPs, guidelines that are issued by the CEO of the
National Health and Medical Research Council which relate to the
use and disclosure of health information for the purposes of
research, or the compilation or analysis of statistics, relevant to
public health or safety. These guidelines sit side-by-side to (and
not in place of) the Privacy Act and APPs. The most recent
guidelines were published in 2014.

In addition, the Productivity Commission identified in its recent
report on Data Availability and Use that there is a need for better
guidance on robust de-identification. The final report of the
Productivity Commission was issued to the Commonwealth
Government on 31 March 2017, and was released publicly on 8
May 2017.

Many Australian States have a health records statute, or a
Corresponding privacy statute which incorporates obligations
about collecting, handling and providing access to health records.
Generally, these statutes impose similar obligations to the Privacy
Act, in that notification or consent of the individual is required for
collection of health information; and destruction or de-
identification of health information on end-of-useful-life of the
information.

New Zealand (NZ) similarly has a Health Information Privacy Code
which falls under the ambit of the NZ Privacy Commissioner’s
regulation. Generally the rules are similar to those in Australia: an
organisation must notify an individual prior to collection of health
information. When health information is no longer required, it
must be transferred or destroyed in a manner that ensures its
confidentiality.

Re-identification – what happened?

The difficulty of successfully de-identifying information was
demonstrated in September 2016. Researchers from the
Department of Computing and Information Systems at the
University of Melbourne were able to re-identify certain de-
identified PBS and MBS data published on data.gov.au (Sample
Health Data). The Sample Health Data constituted 10 per cent of
the MBS data collected between 1984 and 2014 and separate PBS
data collected between 2003 and 2014. The data included in the
set was selected randomly.

The identity of individuals associated with Sample Health Data
was guarded in several ways:
• not including any names or addresses of doctors or patients;
and
• encrypting the identification numbers of doctors and
patients.

Details of the services provided were not encrypted. Partial
details of the encryption algorithm used to de-identify
the identification numbers of doctors and patients was also
published.
The researchers set about analysing the Sample Health Data with the aim of:

‘understanding mathematical facts about encryption and anonymization, in order to ensure that the security of government data is preserved in the face of inevitable efforts of external parties who may be prepared to break the law and attempt to re‐identify the data’.

The researchers used cryptographic methods to reverse the encryption algorithm used to de‐identify doctor identification numbers, and were able to re‐identify the doctor identification numbers (Reidentification Event). The researchers are reported not to have sought to re‐identify the patient identification numbers.

The researchers notified the Commonwealth of the vulnerability on 12 September 2016; the data set was immediately removed from data.gov.au and the OAIC was notified. The OAIC has commenced an investigation to assess whether any personal information is or was at risk, and assess the adequacy of the process to de‐identify the personal information it published. The outcome of this investigation will be made public upon its conclusion.

A swift legislative response

The Attorney‐General announced proposed amendments to the Privacy Act on 28 September 2016 and on 12 October 2016 the Privacy Amendment (Re‐identification Offence) Bill 2016 (Bill) was introduced into the Senate. The Bill creates the following new offences:

• the intentional re‐identification of de‐identified personal information made available by a Commonwealth agency; and

• the intentional disclosure of re‐identified personal information.

Data.gov.au publishes government information for both Federal and State governments, however the Bill relates only to information made available by Commonwealth agencies. In most States there is a separate privacy law applicable to State agencies. At present, no State has proposed an equivalent amendment to the Federal Bill.

Significant sanctions will apply to contraventions, both criminal (up to 2 years imprisonment and/or a fine of up to $21,600) and civil (up to $108,000).

The Bill also introduces offences of counselling, procuring, facilitating or encouraging another to reidentify de‐identified personal information.

The Bill creates an obligation on an entity whose de‐identified personal data has been re‐identified to:

• notify the responsible Government agency of the re‐identification, and

• comply with any directions from the agency about handling of the information.

Civil penalties have been proposed for failures to notify breaches and in this case, the Australian Information Commissioner has jurisdiction to investigate the matter.

The Bill has a different focus to most other provisions of the Privacy Act, which apply only to ‘agencies’ and ‘organisations’, as defined by the Privacy Act. The Bill applies to individuals and small businesses, but does not apply to ‘agencies’, Commonwealth contracted service providers, entities that enter into agreements with agencies, and entities exempted by the Minister.

The amendments to the Privacy Act recognise that de‐identification techniques may become susceptible to re‐identification in the future and so there is a need to develop a network of non‐technical data protections which support technical de‐identification.

If passed, the provisions in the Bill may provide a deterrent against attempted re‐identification, however there are some obvious limitations; an attempt must first be identified before an offence can be alleged and it is possible that re‐identification may occur without ever having come to light (recall that the researchers at the University of Melbourne voluntarily informed the OAIC and the Department). There will also be practical difficulties in enforcing the proposed legislative provisions on persons situated outside of Australia.

The Bill was the subject of a review and report by the Legal and Constitutional Affairs Legislation Committee (Committee), which received submissions raising the following concerns:

• that the risk of re‐identification of government data sets may be too great to warrant releasing them,

• that criminalising re‐identification activities may not be equitable and/or proportionate to other offences contained in the Privacy Act,

• that the offences proposed by the Bill are framed too broadly,

• that the Minister’s power to exempt entities from the offences contained in the Bill are too broad,

• that retrospective operation of the Bill may not be appropriate,

• that the burden of proof to demonstrate that an exemption applies may not be appropriate.

The OAIC has also suggested that it is the responsibility of Government agencies to strengthen their management of privacy risks.

Nevertheless, the majority of the Committee recommended the Bill be passed. In dissent, the Labor and Greens senators argued that the Bill does not provide an appropriate balance between the need for privacy and the need to encourage research into areas including information security, cryptography and data analysis. Rather, they argue, it shifts the responsibility for protecting the privacy of individuals the subject of such information away from government agencies. The Labor and Greens senators also expressed concern about the retrospective application of the Bill. On balance, they recommend that the Bill not be passed.

The Bill is presently before the Senate, and has not yet been presented to the House of Representatives.

The NZ Privacy Commissioner recommended amendments to the New Zealand Privacy Act (NZ Privacy Act) in a report released on 3 February 2017, including protections against the risk of re‐identification of personal information.

In contrast to Australia’s approach of criminalizing re‐identification, the NZ Privacy Commissioner instead recommended:

• the addition of a privacy principle setting out limited circumstances in which re‐identification of de‐identified
Information can occur, to give individuals a right of action where harm is caused by the re-identification,

- the addition of provisions in the NZ Privacy Act which clarify the obligations of agencies in undertaking de-identification activities.

**Implications for healthcare**

The trust and confidence of citizens is key to unlocking the potential of big data in delivering enhanced health outcomes and system sustainability.

The Re-identification Event highlighted potential weakness in the method of de-identification and the security with which de-identification processes are guarded. The legislative response in criminalising de-identification of certain data may have some deterrent effect, however that alone will be insufficient.

Robust and secure de-identification techniques, in conjunction with legal, policy and contractual controls, deployed across government and continually refined in response to changes in technology and approaches, are also needed.

In determining the appropriate portfolio of technical de-identification methods and non-technical governance controls, it is important to assess the risk of re-identification having regard to matters such as technology and the amount of information, along with the need to retain detail in the data for it to be useful for research purposes.

The potential benefits of big data in healthcare are growing as sources of information expand. The change to an ‘opt out’ model for the My Health Record is designed to ensure this becomes a ubiquitous part of the health administration system. The uptake in wearable devices raises the prospect of has opened the door to even richer, real-time, insights to assist people in managing their own health and fuelling innovation in the delivery of services. The continued development in this area is dependent upon public trust in the privacy of personal information.

A 2016 survey by Research Australia found that 90 per cent of respondents were in favour of sharing deidentified health data to advance medical research and patient care. This insight shows that Australians are aware of the benefits that greater use of health data can deliver, but not at the expense of putting their personal information at risk.

**The takeaway**

Protecting personal health data requires a holistic approach, encompassing technical, legislative and process elements, which is difficult, but not insurmountable. The deterrent impact of the Bill has a role to play, but is not a complete solution.

NZ provides an example of a different model to resolve the tension between privacy and access to data. The Integrated Data Infrastructure (IDI) is a large research database containing microdata about people and households, and housing data from a range of agencies, including health information for the NZ population. Access to IDI requires an application and will only occur after the application has been assessed and the ‘five safes’ have been met:

- Safe people – referee checks, signed secrecy declarations and strict protocols,
- Safe projects – must have statistical purpose and be in the public interest,
- Safe settings – access only permitted in secure environment with no external connections,
- Safe data – de-identification and encryption is used rigorously, and
- Safe output – output must be made confidential before release.

Elements of this model could be adopted by Australian Governments to establish a more comprehensive approach, which includes:

- consistent application of robust de-identification methods, supported by advice and guidance from the OAIC and relevant statistical agencies, to promote better practice methodology,
- appropriate security of de-identification techniques and process of continual refinement to ensure that techniques continue to keep pace with new approaches,
- consideration of applying restrictions to access to data.gov.au along the lines of the NZ model,
- greater oversight of use of information and contractual mechanisms which limit the use and distribution of data and re-identification,
- providing researchers with analysis of data, rather than providing access to it, for example, running an analysis of the data and providing the result rather than the raw data,
- greater consumer/community education of and engagement with the potential benefits of big data, and
- strong legislative deterrence.

The selection of appropriate model elements is a manifestation of the tension between freedom of access and innovation and privacy, which is a societal choice that will need to be made by political leaders and supported by informed consumers (who are the data subjects). It would be useful for there to be a consistent approach across the country, which may mean that this is best resolved by the Council of Australian Governments.

The Re-identification Event highlights the challenges of de-identification of data to enable the promise of big data to be realised. It provides a timely call to action to develop a more comprehensive and risk-free approach to de-identification which extends beyond legislative deterrence, and which will ultimately help secure vital trust and confidence of citizens.
DON JUAN AND PROTECTING REPUTATIONS IN AN OPEN DATA ECONOMY

Marta Ganko
Director and National Privacy and Data Protection practice, Deloitte

Ilana Singer
Privacy and Data Protection Specialist, Deloitte

Open data is a bubbling discussion topic in Australia. The Productivity Commission has issued its report into Data Availability and Use, and the Government has made a budget announcement indicating the intention to implement an open banking scheme. Further abroad, in the European Union and the UK, preparations are well under way for open data regulations that are about to come into effect.

The opportunities that open data or data portability will present are not without key challenges that organisations will need to work through as we approach a real-time risk management environment. A successful open data economy that maintains trust with customer will need to be underpinned now, not only by a solid privacy and data management framework, but also risk framework that can identify and manage these risks in real-time. However, the key challenge will be helping customers understand the benefits as well as the risks of an open data economy – given the potential to give away data in the space of seconds.

The following script was presented at the Data + Privacy Asia Pacific Conference 2017 in Sydney on 12 July 2017. Through a story about Don Juan in the digital age, the script highlights what should be done to secure customer confidence and loyalty when organisations share information with one another.

That is:

1. Revolutionise customer confidence through transparent information handling practices.
2. Shield customer data to advantage the customer (e.g. privacy by default).
3. Collaborate with third parties and the customer to share the risks.

As organisations are increasingly seeing the benefits of an open data economy, it is important that they embed customer-centric privacy practices into the fabric of their cultures.

Script

So, who is Don Juan? Don Juan is a legendary fictional libertine, created in 1630 by Spanish dramatist Tirso de Molina. Don Juan prides himself for being famous for his mastery in seduction, while being able to maintain an air of mystery.

The tale of Don Juan has captivated global culture for the past four centuries. Today, our story of Don Juan, in the digital age, will provide the context for our key messages that reflect a need for organisations to not only protect their own reputations, but also that of their customers. How can you, as organisations, do this? Through understanding and respecting your customers’ expectations around privacy, whilst striving to achieve your commercial objectives.

The next 10 to 15 minutes is definitely not about applauding Don Juan’s practices; it’s about understanding the consequences to Don Juan if his expectations of how his data will be used to protect his own reputation are not met. Don Juan will need confidence in our digital age that his data are being protected like one of his treasures, he understands with whom his information is being shared, and that he is told when something goes wrong so that he can start protecting his reputation of mystery.

Our story starts with Don Juan. However – it is not 1630, but 2017, and he does not live in Spain, but here in Sydney, Australia.

Like the fictional character, Don Juan’s sole ambition in life is to seduce many women, needing a level of anonymity to conduct his affairs.

He likes to buy these women flowers, chocolates, and a variety of other gifts. He purchases flowers exclusively at Flower Po, an online Flower Shop.

Don Juan trusts Flower Po because of its transparency over its information handling practices when it:

- collects his contact details; and
- saves his purchasing habits.

This trust is important. Why?

- For Don Juan, it is because he does not want the women he sends flowers to know his home address or that he’s bought flowers for other women.
- For Flower Po, trust with their customer Don Juan has translated into loyalty.

Over the years, Flower Po has collected a lot of valuable information about its customers, including Don Juan. It has been vital for the business to ensure his information is managed and protected in accordance with his expectations, particularly as he is a regular and loyal customer.

Flower Po has realised that the information it holds could be used to drive further loyalty from Don Juan, as well as present a new stream of revenue for the organisation. Flower Po is now seeking to create a loyalty program with partners such as The Online Chocolate Shop.

Don Juan considers signing up. Not only could he now send flowers, he could also earn points and send free chocolates with the points that he earns.

But wait – he thinks – what will The Online Chocolate Shop know about him? He knows his information is in safe hands with FlowerPo, but he doesn’t know whether the Online Chocolate Shop would protect his information to the same degree.

Don Juan does trust Flower Po though.

Flower Po clearly indicates at the point of transaction the type of information that will be shared with The Online Chocolate shop:

- Delivery address
- order number
• and product are required, as the order will still be received from Flower Po.

With this clarity, Don Juan decides to accept the offer, agreeing to disclose this information to The Online Chocolate Shop.

He is confident that as his name is not going across, his privacy and reputation should be safe, as would Flower Po’s.

As you can see, the offer was a success because:
• Flower Po is only sharing the information with its loyalty program partners as is required, and
• Dynamic consent was obtained at the point of transaction, to engage the customer in a decision about how their personal information should be used.

Months go past and Don Juan’s game has lifted – he is able to send bigger gifts for the amount he pays and, even better, he now earns loyalty points from his spending.

All of a sudden, a new digital platform player enters the Australian market. Zappler is a new online business revolutionising flower delivery in Australia. It’s not a flower shop, but a platform to enable any flower shop to deliver flowers. Not only do individuals have more choice, the cost is cheaper as Zappler recommends flowers available closer to the receiving address. Don Juan has a dilemma – this is fantastic, but how will he know which flower shops his details are going to? There is a risk that his data could fall into the wrong hands, which could lead to an unravelling of his reputation of mystery.

Don Juan decides to test Zappler out. As he is unsure and would like to protect his reputation, he registers himself using a pseudonym but a real address.

Zappler makes it easier for individuals to become customers – if information is provided from other online flower shops, Zappler will recreate the orders and delivery addresses in the account without having to type them in again.

Don Juan, of course, has far too many saved addresses to remember.

He provides his Flower Po username and password to Zappler to access and send over his Flower Po orders and delivery addresses.

What are the consequences?
• First, Don Juan’s identity can be revealed by Zappler, now that there is an address to re-identify him with
• Secondly, Don Juan does not realise he can be re-identified
• Thirdly, Flower Po did not consider that sharing Don Juan’s recurring orders was revealing his identity. One organisation has created a risk for another.

At this rate, if Zappler has a data breach, the reputations of FlowerPo, Zappler and, most importantly, Don Juan as the customer, are at risk.

So what can our story of Don Juan teach us about protecting reputations?
• First, our goal should be to Revolutionise customer confidence – we want customers like Don Juan to understand how their information will be used and shared. This transparency and choice will be the incentive that Don Juan needs to accept future information handling requests.
• Secondly, we want to ensure that we advantage the customer by Shielding their data. For example, by making their privacy a default. Don Juan has a specific need for privacy. We don’t always understand why data are important to our customers but this makes it more important to assess the potential risks of sharing and using specific data assets.
• And finally, we should Collaborate – work with our customers and third parties to share decision making throughout the lifecycle of data management. Collaboration is an opportunity to share control and the risks with Don Juan. Whilst this creates an additional responsibility for organisations, it allows them to relinquish partial control of information held and hence the risk.

These three approaches will be beneficial not only to the customer but for the businesses too.
As the Lead of Deloitte’s National Privacy and Data Protection practice, I see the challenges outlined in this story playing out across many industries in Australia. In particular, the challenges that we are helping our clients most with, on top of traditional privacy advisory and implementing frameworks and training and awareness plans, see our work now being focused on developing open data strategies and implementing consent management, de-identification and more recently API management solutions.

These are not just challenges here in Australia but in other parts of the world too. Regulation has already been introduced that is encouraging organisations to challenge existing data protection practices, such as the EU GDPR and Payment services Directive in Europe. So we are not alone.

In some respects Australia is slowly catching up, with the release of the Productivity Commission’s report into data availability and use, and the budget announcement around the introduction of an open banking scheme. In many ways, in this new data fuelled industrial revolution that’s underway, we are all in the same boat.

We are all operating like startups – figuring out how to operate in this world where so many stakeholders have varying expectations such as Regulators, partners, vendors and, most importantly, customers such as Don Juan, many of whom having unique expectations. What this means in practice is that this is now anyone’s game – and a large opportunity for organisations to build trust and a reputation in the market for consumer-centric data management by, as mentioned before:

- Revolutionising customer confidence
- Shielding customer data
- …and Collaborating to share risk.

ABOUT THE AUTHOR – MARTA GANKO

Marta leads Deloitte’s National Privacy and Data Protection risk practice in Australia. Marta has a unique combination of skills including business analysis, technology delivery, as well as privacy regulatory knowledge. She has a passion for educating both consumers and organisations regarding privacy risks and provides a customer-centric view to privacy. In her career, she has served clients across the Financial Services, Telecommunications and the Not for Profit sectors. Marta leads several privacy initiatives including Deloitte Australian Privacy Index that has received national media attention. She can be contacted at mganko@deloitte.com.au.

ABOUT THE AUTHOR – ILANA SINGER

Ilana is a Senior Analyst and Privacy and Data Protection Specialist in the Cyber Risk Services practice. Before joining Deloitte, Ilana worked at the Office of the Commissioner for Privacy and Data Protection. Ilana brings experience and expertise in understanding the privacy and data protection regulatory landscape, and delivering tailored solutions that meet compliance obligations while supporting organisation strategy. She can be contacted at isinger@deloitte.com.au.
EVENT CALENDAR - METADATA & THE PRODUCTIVITY COMMISSION REPORT - PANEL DISCUSSION

Courts in many jurisdictions, including recently the Australian Federal Court, are being asked to interpret the meaning of personal information. Technology is enabling organisations to collect and use more and different data about a range of subject matters, including individuals, for various purposes.

Considering the Productivity Commissions report we will reassemble the panels to address the following in relation to personal data:

- The key findings of the Productivity Commission’s report
- implications for privacy protections and privacy professionals
- how does the Australian experience compare with similar economies in the EU or Asia?
- what is next from the industry perspective
- what is next from a regulatory perspective

SYDNEY

Date: 21 August 2017
Time: 5:30pm – 8pm
Venue: Gilbert + Tobin
International Towers, Tower 2/200 Barangaroo Avenue, Sydney
Cost: FOC for members | $49 for non-members

REGISTER HERE

MELBOURNE

Date: 22 August 2017
Time: 5:30pm – 8pm
Venue: PwC
2 Riverside Quay Southbank VIC 3006
Cost: FOC for members | $49 for non-members

REGISTER HERE

BRISBANE

Date: 23 August 2017
Time: 5:30pm – 8pm
Venue: Corrs Chambers Westgarth
42/111 Eagle St, Brisbane City QLD 4000
Cost: FOC for members | $49 for non-members

REGISTER HERE
EVENT CALENDAR - PRIVACY AFTER HOURS

Privacy After Hours is the iappANZ networking event series which runs regularly across Australian and New Zealand capital cities throughout the year and is open to all members and sponsors to attend (free of charge!).

Please find details and the registration link below to upcoming networking events, we look forward to seeing you after work for a drink or two in Melbourne, Sydney or Brisbane.

MELBOURNE
Date: 14th of September 2017
Time: 5:30pm-7:00pm
Venue: Mr Mason, Melbourne
Cost: Free of Charge for members

REGISTER HERE

BRISBANE
Date: 14th of September 2017
Time: 5:30pm-7:00pm
Venue: Buffalo Bar, Brisbane
Cost: Free of Charge for members

REGISTER HERE

SYDNEY
Date: 14th of September 2017
Time: 5:30pm-7:00pm
Venue: Palings Kitchen, Sydney
Cost: Free of Charge for members

REGISTER HERE

iappANZ 2017 Summit
Privacy & personalisation: walking the line

Tuesday, 3 October 2017
Dockside, Cockle Bay Wharf, Sydney, NSW

EARLY BIRD ENDS 16 AUGUST 2017
Registration is now open for the annual iappANZ Summit. We look forward to seeing members in Sydney for what promises to be an interesting and insightful day of walking the line between privacy and personalisation.

Speakers and program to be announced in the coming weeks.

REGISTER HERE
University Complaints and Information Access Officer

University of Newcastle

- Use your excellent interpersonal and problem solving skills in this role
- Assist the Assurance Services team to provide an excellent service
- Full-time, continuing opportunity
- Use your GIPA and privacy knowledge to implement sound frameworks and practices.

Vice-Chancellor's Division - Assurance Services

University Complaints and Information Access Officer 3373

About UON

Be part of a university on the move. Building on strong foundations, we are ranked well within the top 250 universities worldwide in the QS and Times Higher Education ranking systems. The strength of UON’s foundations allow us to focus firmly on the future. UON invites you to consider joining our university - where curious and courageous minds collaborate to write the future for our university and the world. Your contribution to making us a world-class institution is recognised and rewarded in many different ways. Competitive salaries, formal awards programs, development opportunities and promotions are just the start.

About the opportunity

The role is to ensure that the planning, design, conduct, management and reporting of complaints, information access and compliance activities support the identified risks.

This role requires knowledge and experience in complaint handling processes and in the management of requests for information in line with statutory obligations. The role requires the ability to effectively engage with and respond to requests in a timely and effective manner, managing and maintaining working relationships and providing timely and accurate information and reports in accordance with regulatory and operational requirements.

Other key responsibilities include:

- Providing a responsive and effective complaints, information access and privacy protection service;
- Effectively managing, investigating and resolving as able and report with clarity on the outcomes of complaints and information requests;
- Working productively across multiple services and campuses and with statutory agencies;
- Training and educating staff and students in the implementation of relevant legislative, policies, processes and practices; and
- Continuously improving relevant processes and practices;

Skills and experience

This role requires well developed interpersonal skills. Knowledge and understanding of complaints, compliance, public information access and privacy protection processes. Be able to work effectively within a team environment and acting in a highly professional manner. An ability to resolve problems, taking into account a range of technical and policy requirements while managing competing priorities and timeframes.

For the full list of selection criteria, please access the position description on the UON website - Job Vacancies.

Please note: In accordance with the University’s Staff Selection Guidelines, your application will be assessed on the selection criteria. It is essential that you address each of the criteria to enable the selection committee to properly assess your application and suitability for interview.

APPLICATIONS CLOSE: MONDAY 21 AUGUST 2017 AT 11.55PM.

HEW 7 - 84,302 - $94,839 + 17% superannuation.

Contact person: Bruce Devonport, Senior University Compliance and Privacy Officer 02 4921 5927 or Bruce.Devonport@newcastle.edu.au