MATRIXCNI
COMPLETENETWORKINNOVATION

Re-thinking data collection, storage and security in an IoT world

Does improving customer experience change the way we think about privacy?

The Internet of Things (IoT) changes everything. The rise in IoT devices that collect data about you from smartwatches, home speakers, home automation and smart TV's through to cell tower logging and browsing history collection creates a new world that redefines privacy.

This pervasive data collection enables analysis previously unimaginable and can be harnessed to enable new levels of personalised service.

It does though mean that previous concepts of privacy need to be reimagined when your every move is generating trackable data.

It is not alarmist. It is not a call for a retreat to a rose-coloured past with greater control over privacy. It is though, a sobering reality worth considering to ensure appropriate controls are in place.

With so many devices collecting and using the data we generate in our daily lives do we really understand who can access that data and how it can be used? Does anyone read the privacy statement or T&Cs of these devices or apps before they install them? The intent of course is to improve the delivery and relevancy of services – that's why the data is collected.

The massive uptake of these devices suggests that most people don't mind sharing personal data when it's used well – even if that purpose is marketing. People have voted with their feet, wrists and dollars. Personalised customer experiences are valued and to many are worth the trade-off in privacy.

That trade-off isn't universal though. When your personalised data is then accessed without authorisation or is sold to third parties with less honourable intent suddenly public perceptions change. What was assumed to be innocent data sharing can suddenly appear invasive and even abusive.

So where do we draw the line and how can organisations deliver personalised customer experiences without crossing the line under the law and under the harsh gaze of customers?

Is your business subject to Australia's Privacy Framework?

The short answer is, yes. Your organisation is almost certainly subject to aspects of the framework.

The Australian Privacy Principles (APPs), which are contained in schedule 1 of the Privacy Act 1988 (Privacy Act), outline how most Australian and Norfolk Island Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses (collectively called 'APP entities') must handle, use and manage personal information. Even if your organisation doesn't fit any of the above criteria, you still need to be incredibly careful about the collection of personal data and can easily run afoul of privacy requirements if you buy, sell or use personal data in ways that your staff and customers have not authorised.

Understanding the Australian Privacy Principles

While the Australian Privacy Principles are not prescriptive, each APP entity needs to consider how the principles apply to its own situation.

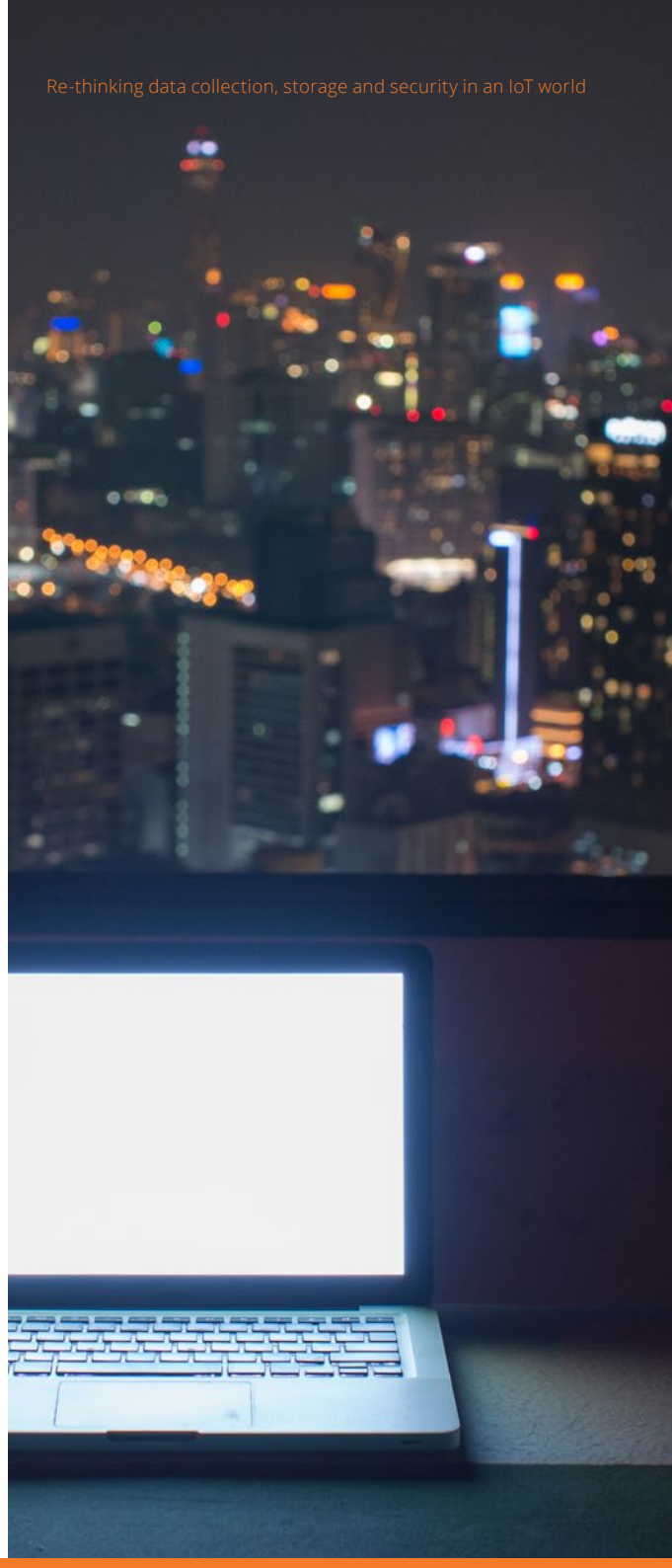
The principles cover:

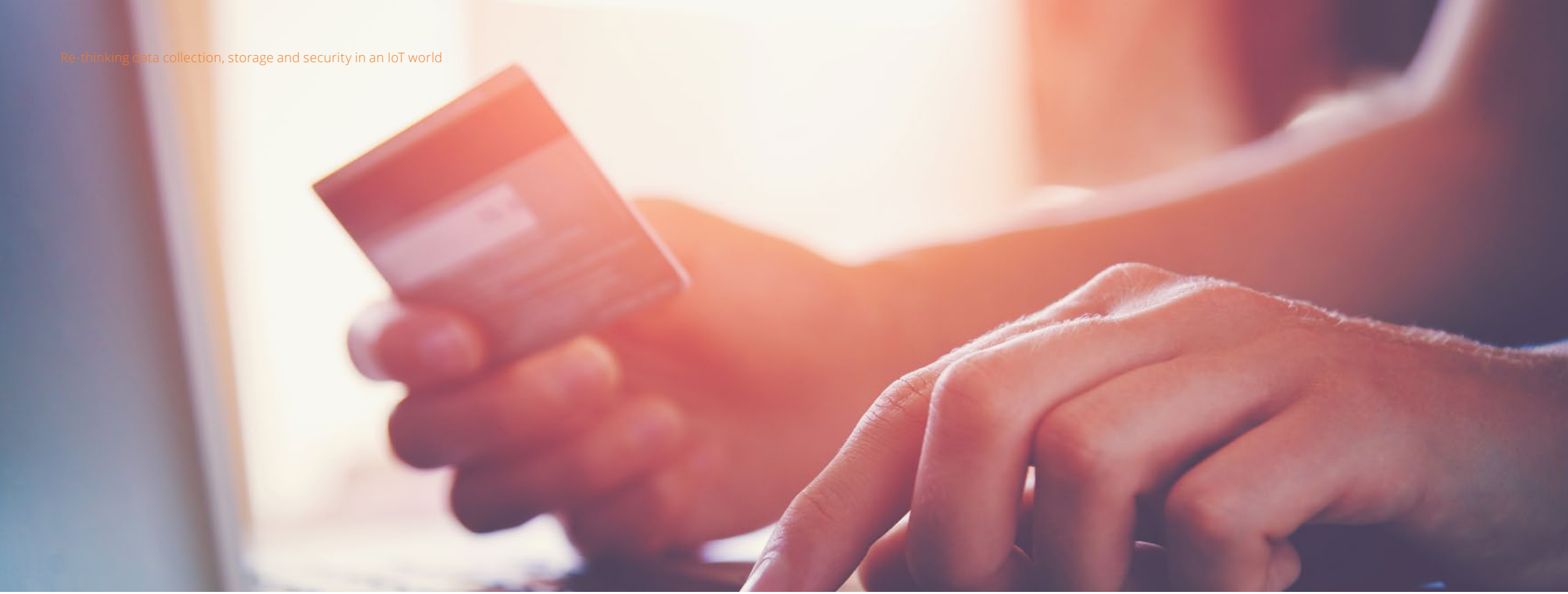
- Open and transparent management of personal information including having a privacy policy
- Individuals having the option of transacting anonymously or using a pseudonym where practicable
- Collection of solicited personal information and receipt of unsolicited personal information including giving notice about collection
- How personal information can be used and disclosed (including overseas)
- Maintaining the quality of personal information
- Keeping personal information secure
- Right for individuals to access and correct their personal information.

There are also separate Australian Privacy Principles that deal with the use and disclosure of personal information for direct marketing, cross-border disclosure of personal information and the adoption, use and disclosure of government related identifiers.

The APPs place more stringent obligations on APP entities when they handle 'sensitive information'. Sensitive information is a type of personal information and includes information about an individual's:

- Health (including predictive genetic information)
- Racial or ethnic origin
- Political opinions
- Religious beliefs or affiliations
- Membership of a political association, professional or trade association or trade union
- Philosophical beliefs
- Sexual orientation or practices
- Criminal record
- Biometric information that is to be used for certain purposes
- Biometric templates.





Is your organisation ready for mandatory data breach reporting?

You may not be aware yet, but your obligation as an organisation to protect personal data has recently been extended to an obligation to rapidly notify and advise people whose personal data privacy may have been breached.

The Privacy Amendment (Notifiable Data Breaches) Act 2017 established a Notifiable Data Breaches (NDB) scheme in Australia.

The Notifiable Data Breaches scheme requires organisations covered by the Australian Privacy Act 1988 (Privacy Act) to notify any individuals likely to be at risk of serious harm by a data breach.

This notice must include recommendations about the steps that individuals should take in response to the data breach. The Office of the Australian Information Commissioner (OAIC) must also be notified.

Organisations will need to be prepared to conduct quick assessments of suspected data breaches to determine if they are likely to result in serious harm.

A data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure. So, if you lose a device containing customers' personal information, a database is hacked or you intentionally or mistakenly provide personal information to the wrong person your organisation needs to take immediate action.

So, what exactly is personal data?

A landmark case in the Federal Court significantly narrowed the definition of personal data in January 2017, but the subtleties of that narrowed definition require careful attention by organisations that collect data about customers and staff.

While data privacy laws protect "personal information" in which a person is identified or identifiable from data, the 2017 court decision means "personal information" may not include data that only reveals identity if it is subsequently linked with other data.

Think about using your smartphone. Cell towers log information about you as you move about, information that is stored and used for a number of purposes including traffic and capacity management.

While that information contains specific identifiers for your smartphone, according to this latest court decision, it doesn't constitute personal information. This is because this cell tower data would need to be managed with your telco's billing system to be able to associate it with your name, address, etc. Without that matching, it's effectively anonymous.

Where collected data meets this criterion, it is not subject to any restrictions on processing or disclosure to other entities. However, organisations need to be very careful to ensure they don't inadvertently cross this line.

Clearly, the issue of de-identification and anonymising of data becomes critical. So too does an understanding that they are not the same thing. Each organisation needs to have a clear understanding of what is justified in their specific context. This is important because the Privacy Act sets out principles, not specific prescriptions.

So, decisions on whether your organisation is compliant often depends on the context of your organisation, how and why you collected the data, and the reasonableness of the steps that you have taken to protect the data in that context.

Extract from 2016 speech to CEBIT by Timothy Pilgim PSM, Australian Information Commissioner and Australian Privacy Commissioner

"As our digital touch points increase, and the Internet of Things becomes more and more embedded in our everyday lives, the data we create becomes increasingly valuable. Valuable to both private and public sector alike.

Done correctly, de-identified information is no longer personal information and is therefore outside the scope of the Privacy Act.

But what does "done correctly" entail?

De-identified means de-identified in whose hands?

And in what use?

If I am the collector of the personal information, am I obliged to have regard to the re-identification potential of data in its current context, the next foreseeable context, or any context?

And what about the ability of data analytics to create entirely new and personal information — raising the prospect of an entity effectively collecting new personal information by creating it?

These are all pertinent questions, but if you think I'm going to give clear and simple answers now, then I'm afraid you are in for disappointment.

This is for a good reason. Namely, the Privacy Act is principles, not prescription, based, and ultimate answers as to compliance with it will often be bespoke to the circumstances.

This is certainly true if your preferred solution to privacy governance is de-identification. The specific changes required to your data set will arrive as the result of a risk based assessment of the data's potential use, disclosure and re-identification prospects.

While the principles remain constant — and are already covered in our existing guidance on information sharing and de-identification — the solutions executed are often bespoke to the data and its intended use."

Third party data hosting and storage
whose rules apply?

The Internet of Things is a quiet revolution that is rapidly transforming the way we live, work and play. It is a change of magnitudes that most people remain oblivious to. Yet it is happening and the speed of change is accelerating. It is transforming marketing, service delivery, supply chains and asset maintenance. Where though is that massive explosion in data going to be stored and analysed? The sheer volume of data being generated is staggering and continues to increase by previously unimaginable orders of magnitude.

How is personal privacy protected if data is collected and stored by an overseas entity? Who is responsible if there is a data breach? What exposure does your organisation have? Are you adequately prepared for a potential breach? Do you really understand the data sovereignty considerations for every aspect of your organisation's operations?

The fact is, if an Australian company discloses personal information to a company overseas, the Australian entity is ultimately responsible and must take reasonable steps to ensure compliance with the Australian Privacy Principles.

The Australian Privacy Principles acknowledge that de-identification of personal information may be more appropriate than destruction where the de-identified information could provide further value or utility to the organisation or a third party.

However, regardless of the de-identification technique chosen, the risk of re-identification must be actively assessed and managed to mitigate this risk. Where it is not possible for the risk of re-identification to be appropriately minimised, the organisation could instead consider taking reasonable steps to destroy the personal information. Where the personal information is held on a third party's hardware, such as cloud storage, and the organisation has instructed the third party to de-identify the personal information, reasonable steps to de-identify the personal information would include taking steps to verify that this has occurred.

So it is not only a matter of having your own house in order, you need assurance that your cloud providers and other IoT vendors and data hosts are equally compliant and that at the very least, you have clear documentation and procedures in places to minimise and mitigate the risk of any potential data breach.

Extract from Australian Privacy Principles Guidelines, Office of the Australian Information Commissioner

"Taking reasonable steps to destroy or de-identify personal information.

The 'reasonable steps' that an organisation should take to destroy or de-identify personal information will depend upon circumstances that include:

- the amount and sensitivity of the personal information— more rigorous steps may be required as the quantity of personal information increases, or if the information is 'sensitive information' or other personal information of a sensitive nature
- the nature of the organisation. Relevant considerations include an organisation's size, resources and its business model. For example, the reasonable steps expected of an organisation that operates through franchises or dealerships, or gives database and network access to contractors, may differ from the reasonable steps required of a centralised organisation
- the possible adverse consequences for an individual if their personal information is not destroyed or de-identified — more rigorous steps may be required as the risk of adversity increases
- the organisation's information handling practices, such as how it collects, uses and stores personal information, including whether personal information handling practices are outsourced to third parties
- the practicability, including time and cost involved — however an organisation is not excused from destroying or de-identifying personal information by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances.

While Australian Privacy Principle 11.2 requires an organisation to take reasonable steps to either destroy or de-identify personal information, in some circumstances one or the other may be more appropriate."

Conclusion
What should businesses do?

Denial is not an option. Immobilised by the scale of the task is unproductive. And the reality is it is also unnecessary. Yes, there are serious considerations and significant legal obligations, but a careful plan and considered approach can address most of this. The point is you need to be prepared and you need to start now.

Quick questions to guide you on what to consider first:

- Have you clearly documented what personal information your organisation collects?
- Do you have clearly documented procedures to check where and how each new IoT implementation within your organisation impacts data privacy?
- Do you have clear documentation on where that data is stored and how it is protected?
- Are you crystal clear on whether your cloud infrastructure and network architecture adequately protects the personal data you store?
- Have you developed a data breach response plan and is it up to date?
- Do you need to update your organisation's privacy policy?
- Who in your organisation has access to the personal data you store, what controls do you have in place, and are they adequate?
- Can you turn your privacy policies and processes into a competitive advantage?

If you have the appropriate skills in-house, the onus is on your organisation to get prepared and remain prepared. If you don't have the skills in-house, ignorance is no excuse under the law. Find a trusted network and security partner that knows the space well and can help you get your house in order with the minimum of fuss.

Investing to prevent privacy breaches occurring in the first place and to prepare in advance in case a breach ever happens is always more effective than attempting to scramble after the fact.

About
Matrix CNI

Matrix CNI is an Australian owned specialist network integrator with expertise in the fields of Campus LANs, Converged Data Centre Infrastructure, Unified Communications, Wireless Mobility, Application Availability and Data Security. We maintain strategic relationships with a select group of key industry vendors to provide competitive, reliable and secure network solutions with best of breed performance to support a fixed and mobile workforce. MatrixCNI clients include a wide range of education, health, government and enterprise organisations.

MATRIXCNI

MatrixCNI Pty Ltd

13-15 Lyon Park Road
Macquarie Park NSW 2113

1300 850 400 | **info@matrixcni.com.au**