Privacy Impact Assessment Workshop

on behalf of the Office of the Australian Information Commissioner

Facilitated by Anna Johnston

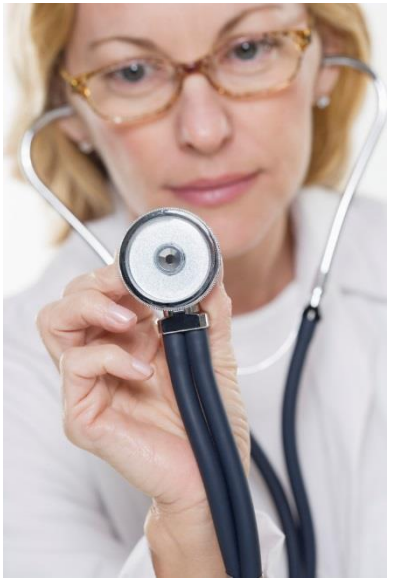
www.salingerprivacy.com.au

Today's session

- **introduction:** what is a PIA? where does it 'fit' in corporate governance? what are the benefits?
- **getting started:** when do we need one? what is the right time? who should do it? what is the scope?
- **the nuts and bolts:** how do we do a PIA? what is involved? how do we identify and mitigate privacy risks?

What is a PIA?

- a diagnosis – a tool to identify the privacy impacts of a *future* project
- and a prescription – a tool to identify ways to minimise the negatives and maximise the positives
- it is *not* the medicine
- nor is it exploratory surgery (audit / assessment) or an autopsy (evaluation)

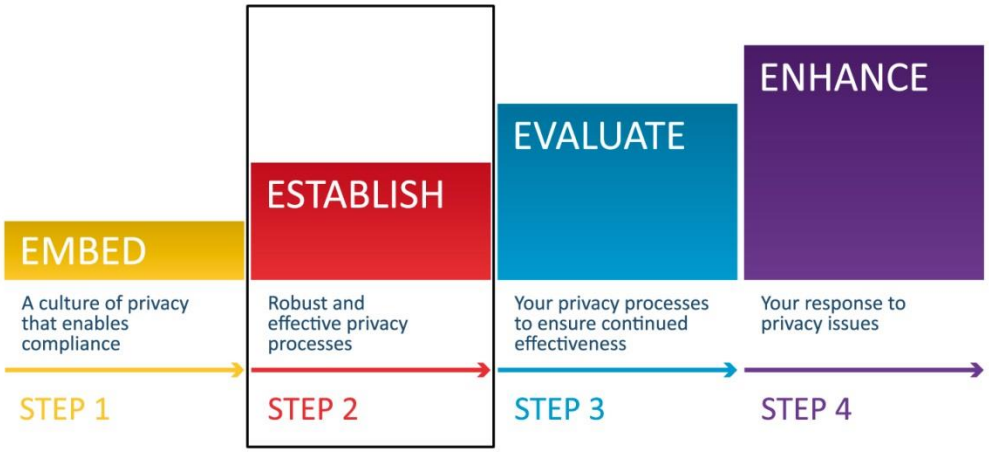


PIA or PbD?

- APP 1.2: “take such steps as are reasonable in the circumstances to implement practices, procedures and systems” to ensure compliance
- Privacy by Design (PbD): a **philosophy** of building-in privacy compliance at the start
- one **tool** to help you meet APP 1 and achieve PbD is the **methodology** of PIA
- the Privacy Commissioner can now direct agencies to conduct a PIA

And now PMF … ?

- *other* tools in your kit should include privacy audits, info security testing, staff awareness, clear policies, etc
- see the new OAIC Privacy Management Framework (PMF) for how it all ties together



Terminology: impact or risk?

- privacy impacts can be positive (privacy-enhancing) or negative (privacy-invasive)
- I use privacy 'risk' to mean the risk that a project:
  - will not comply with privacy laws, and/or
  - will not meet community expectations, and/or
  - will have unmitigated / unnecessary negative privacy impacts on individuals

Examples of privacy 'fails'

Projects canned because of community concerns

- Australia Card
- inBloom, an American non-profit student data repository with $100M in seed funding

Privacy risks not appreciated until too late

- Google Buzz
- NYC taxi data
- the itty bitty change to the database which, oops, results in accidental disclosure

Benefits of a good PIA

- building-in legal compliance and best practice from the start, avoiding costly mistakes
- helps gain public trust and acceptance
- provides innovative business solutions
- forces project team to explain business case in plain language
  - can expose internal communication gaps and hidden assumptions
  - helps you craft your external communication message

Benefits of a PIA program

- “It helps you to identify trends and business-as-usual risks
- As stakeholders get used to the process, they learn more about privacy and hence, start to address privacy problems and design pro-privacy solutions themselves
- It has helped the privacy team to build on its understanding of operational problems and solutions, which enables us to offer a better service to our internal customers.”

(Melanie Marks, Executive Manager Digital Trust & Privacy, CBA)

How? The 10 steps to a PIA

1. Threshold assessment
2. Plan the PIA
3. Describe the project
4. Identify and consult with stakeholders
5. Map information flows
6. Privacy impact analysis and compliance check
7. Privacy management – addressing risks
8. Recommendations
9. Report
10. Respond and review

1: Threshold question

Q: Will any personal information be collected, stored, used or disclosed in the project?

- What is a ‘project’?

- legislation, policy, technology, business process

- Even if ‘no’, might a PIA be a good idea?

- *demonstrate* no personal information involved

- other privacy issues e.g. physical privacy

A: Regardless, document the assessment

2: Plan the PIA

- scope
- timing
- who should do it
- available resources and inputs
- stakeholder consultation
- plans for completion: who to review / approve / respond / implement / monitor

Scope of the PIA

How ‘big’ a PIA do we need? Project size or budget is not a good indicator.

Consider…

- quantity of personal information involved
- type of personal information involved (sensitive? home addresses? geolocation?)
- extent of info sharing between organisations
- likely community interest

What laws?

A PIA should check compliance with:

- the Privacy Act (or your State/Territory equivalent, e.g. Info Privacy Act)
- State/Territory health privacy laws?
- secrecy provisions in your own statutes?
- laws about surveillance, communications privacy, etc?

Timing

- need to have project objectives clear
- point of PIA is to affect the design of the project (before it is too late!) – an iterative method
- ideal time is once you have exec approval for project initiation / business case
- if in doubt, err on side of earlier, and revisit later
- for legislation, a PIA should inform your drafting, and *Stmt of Compatibility with Human Rights*

Who should do the PIA?

expertise: law, ethics, technology, info security, operational / industry knowledge

internal: has the operational / technical knowledge; faster (unless you have other priorities); maybe too ‘close’ to project

external: has the privacy knowledge; brings ‘fresh eyes’ and independence; costs more

Resources and inputs

- any published information
- business case documents
- any existing analysis, legal advice, etc
- first-pass look at systems
- current or draft technical specifications
- stakeholder list and contact details
- research sources on attitudes towards privacy

3: Describe the project

- a ‘big picture’ overview - no analysis yet
- avoid jargon or assumptions - should work as a standalone description for a lay reader
- summarise the business case; IT design; legislation, policies, procedures; how the project is communicated to clients; physical environment and staffing; and accountability mechanisms

4: Identify & consult with stakeholders

- internal stakeholders
- related bodies, including service providers
- clients / customers / the public (and/or NGOs who represent them)
- privacy regulator
- industry experts

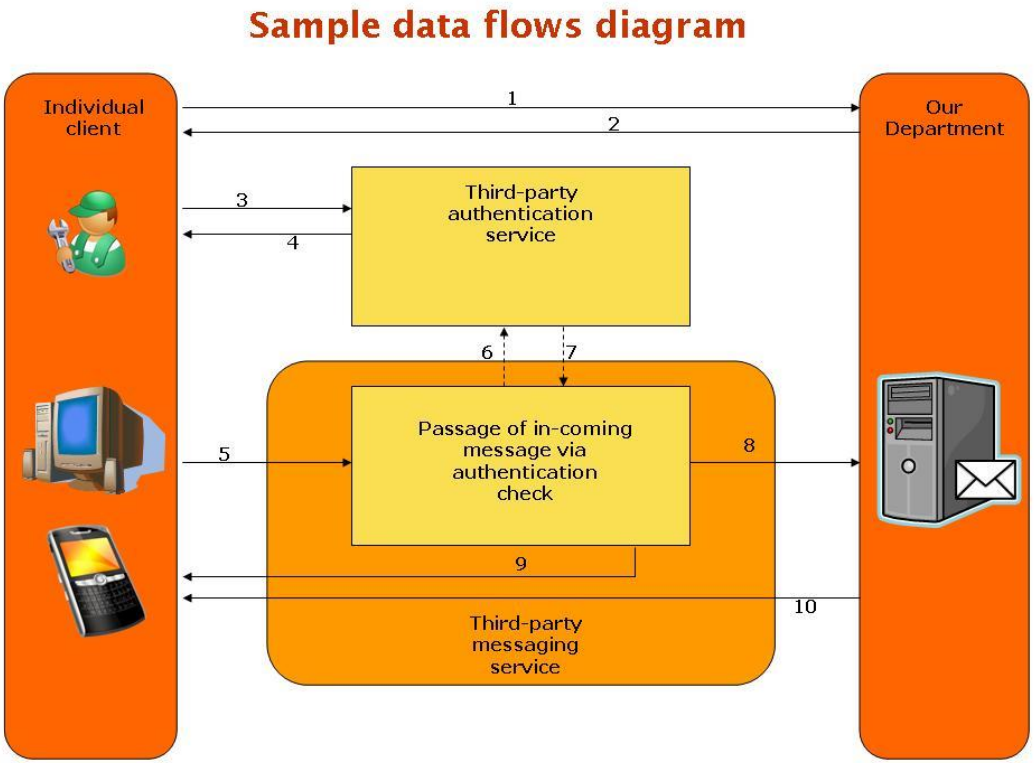
Public consultation benefits

- you'll get a 'heads up' on stakeholder concerns and any 'myths' that need correcting
- identification of risks
- can also help identify or 'reality-test' possible solutions
- offers transparency, and opportunity to influence

5: Map & describe the information flows

- identity verification
- collection
- use
- disclosure
- data quality
- data security; and
- access and correction

Group Exercise 1
Drawing a Data Flow diagram



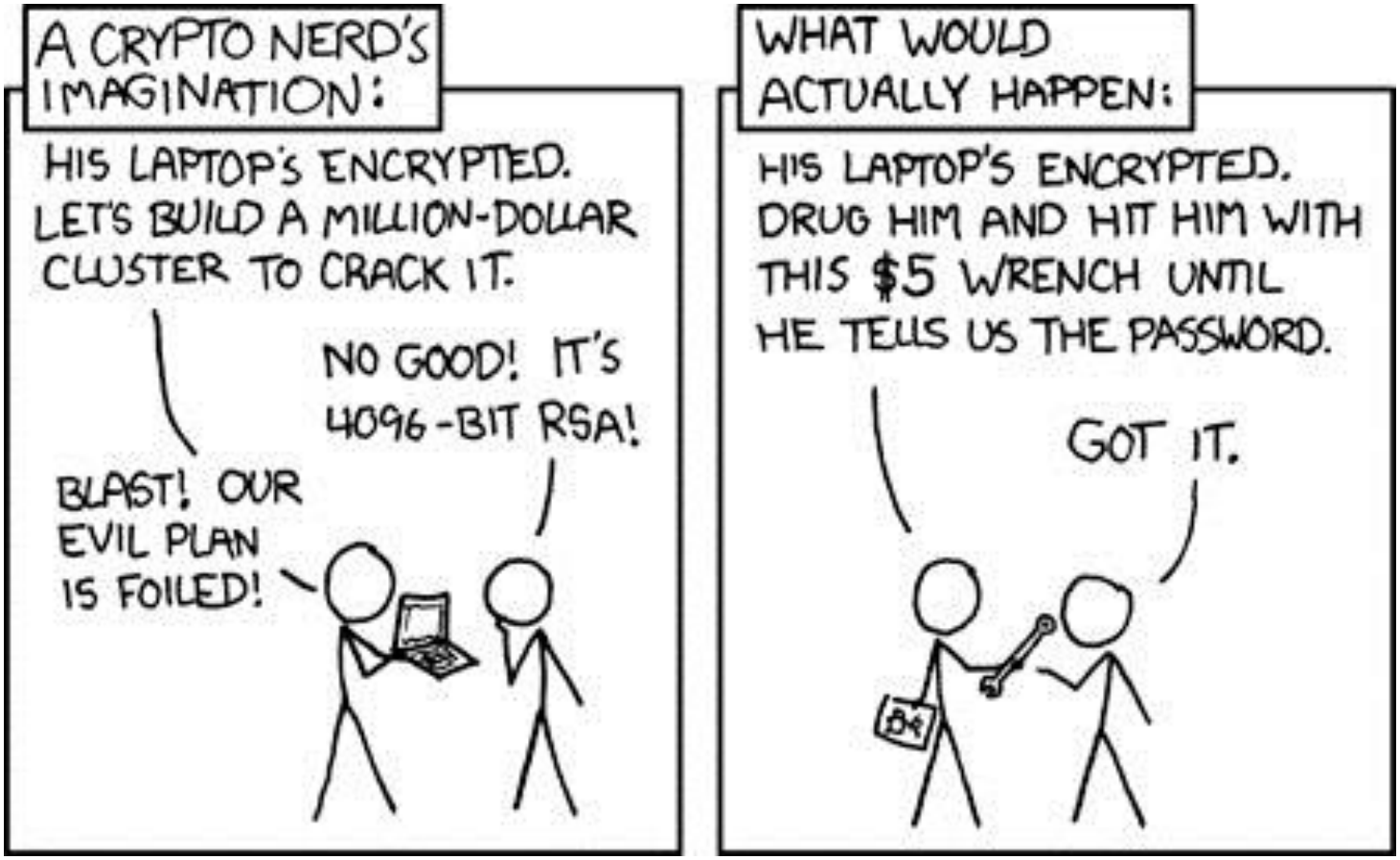
6: Identifying risks

- testing for compliance with the law, but also community values
- structured approach – break it down by APPs
- privacy management of the project: transparency, oversight, accountability, future function creep
- wider privacy control environment: complaint-handling, breach management, staff training

Common privacy risks

- poor justification
- poor design
- failure of technology
- failure of people (human error, ignorance of requirements, or deliberate misconduct)
- lack of transparency

7: Identifying solutions



Mitigation strategies

You can use any of the following levers:

- technology design
- legislation
- policies and procedures
- transparency (internal and/or external communication strategies)
- staff training
- accountability measures

Mitigation starting points

- ensure the project has a sound justification
- minimise the personal information you collect to only what is absolutely necessary
- transparency: do a thorough privacy notice
- limit uses and disclosures
- protect data security
- ensure data quality, access and correction

Group Exercise 2

Identifying risks and solutions

8: Recommendations

- for each avoidable risk: recommendation/s to remove or reduce that risk
- note any remaining risks which will need to be accepted by the entity
- draw a conclusion as to whether the benefits of the project will outweigh those remaining risks – may need to recommend the project not proceed at all

9: Report

- describe the project and data flows
- identify the privacy ‘positives’, and describe each privacy risk:
  - legal non-compliance
  - not meeting community expectations
- note possible mitigation strategies
- recommendations and conclusion

10: Respond and review

- may need to ‘sell’ the recommendations to your team or senior management
- PIA recommendations should feed into project design
- remaining risks should be entered in project Risk Register
- provide PIA Report and Response to stakeholders, regulator … and publish
- consider review / updating

PIA resources

www.oaic.gov.au

- PIA Guide - see Appendix A for references to other helpful resources
- Guidelines on Data Matching
- new Privacy Management Framework
- community attitude surveys over time

www.alrc.gov.au

- ALRC Report 108 – community attitudes

What have we learnt?

- privacy risk is about legal compliance AND meeting community expectations
- a PIA helps you identify the privacy risks that could arise from your project
- and should generate possible solutions so you can build-in privacy protections from the start = PbD, APP 1 compliance
- follow the 10-step process

Thank you

Anna Johnston
Director

SalingerPrivacy

www.salingerprivacy.com.au

on behalf of the

Australian Government
Office of the Australian Information Commissioner