Australian Government
Office of the Australian Information Commissioner

Government data matching and the Privacy Act 1988 (Cth)

Dimitrios (Jim) Kormas | Assistant Director| Privacy Assessments

17 May 2018

Agenda

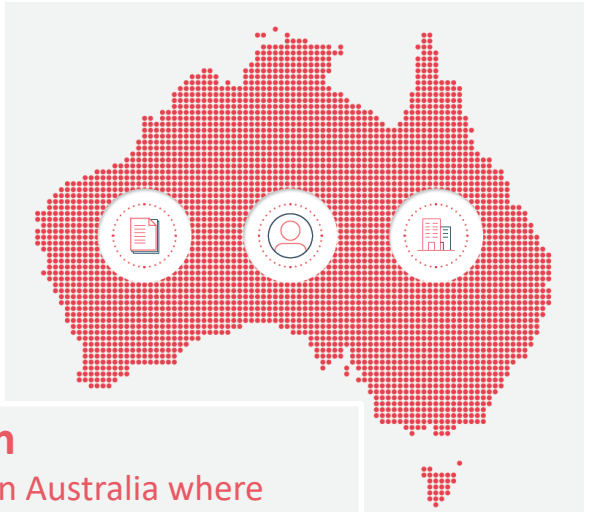
- Brief overview of the OAIC, Privacy Act and Australian Privacy Principles (APPs)
- OAIC's involvement in Government data matching activities
- Key privacy guidance, issues, and ideas for better privacy practice
- Questions

Office of the Australian Information Commissioner (OAIC)

Privacy, FOI and government information policy

Privacy functions drawn from the Privacy Act 1988

Australian Information Commissioner and Australian Privacy Commissioner



OAIC Vision

Our vision is an Australia where government information is managed as a national resource and personal information is respected and protected

What does the Privacy Act cover?

Privacy Act provides for the protection of an individual's personal information

Privacy Act contains provisions that deal with:

- 'personal information'
- 'sensitive information' (such as health information)
- tax file numbers
- credit information

Australian Privacy Principles

13 APPs in total

- Principles apply to Government agencies and private sector organisations (referred to as ‘APP entities’)
- Structured to reflect the information life cycle — planning, collection, use and disclosure, quality and security, access and correction
- OAIC’s *APP guidelines*

OAIC's regulatory and enforcement powers

Regulatory powers

- Conciliate or determine complaints (with compensation)
- Receive / investigate data breaches
- Conduct assessments of entities
- Investigate on own initiative
- Create enforceable codes
- Require Privacy Impact Assessments

Enforcement powers

- Accept an enforceable undertaking
- Make a determination following a complaint or CII
- Bring proceedings to enforce a determination
- Apply to the court for an injunction
- Apply to the court for a civil penalty

What is data matching?

- "The bringing together of at least two data sets that contain personal information, and that come from different sources, and the comparison of those data sets with the intention of producing a match."

  - OAIC's Guidelines on Data Matching in Australian Government Administration

- Data matching can be a valuable data resource for policy, planning, research and innovation
- Building privacy into data-driven innovation can build public trust in how agencies use personal information.

OAIC involvement in data matching

Key OAIC activities relating to data matching include:

- Providing policy advice to agencies conducting data matching activities (voluntary guidelines)
- Providing comments on data matching protocols, and responding to exemption requests, under the voluntary guidelines
- Conducting assessments – e.g. Department of Human Services' data matching activities, specifically funded under a 2015–16 Budget measure.
- Oversight role under the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) and Medicare/PBS under s 135AA of the *National Health Act 1953* (Cth)

Privacy guidance – data matching

Guidelines on Data Matching in Australian Government Administration

- Ensure data matching complies with the Privacy Act, and is consistent with good privacy practice
- Do not generally apply to data matching using TFN information and do not apply to data matching using PBS Medicare information
- Apply to data matching involving more than 5000 individuals
- Voluntary, but taken into account when assessing whether an agency has complied with the APPs.
- Exemptions from the guidelines and regular evaluation

Privacy guidance - data matching

- The OAIC receives new and amended protocols, exemption requests – generally 5-10 per year
- The OAIC provides comments on program protocols
- Before commencing a data matching program, the primary user agency should prepare a Program Protocol and Technical Standards Report
- Public notice
- Do not create new registers, data sets, or databases
- Destroy information no longer required – 90 day retention period
- Publication of protocols and exemption requests
- Undertake a Privacy Impact Assessment (PIA)

Privacy guidance – data matching

Guide to Data Analytics and the Australian Privacy Principles

- Consider risk of generating new information through ‘collection via creation’
- Be open and transparent about your privacy practices
- Consider whether de-identified information may be sufficient
- Know what you’re collecting, why you’re collecting it, and how long you need it for - using ‘all the data’ for ‘unknown purposes’ and retaining it indefinitely will expose your organisation to privacy compliance risks
- Conduct PIAs for your data analytics projects even where using de-identified data

Privacy guidance – data matching

Guide to securing personal information

- Governance, culture and training
- Documented internal practices, procedures and systems
- ICT security
- Access security
- Third party providers (including cloud computing)
- Data breach response
- Physical security measures
- Destruction or de-identification
- Standards (ASD strategies, ISM, PSPF)

Privacy assessments

- Assessment power - s 33C Privacy Act
- OAIC privacy oversight role in DHS data matching activities under the 'Enhanced Welfare Payment Integrity – non-employment income data matching' 2015-16 budget measure'.
- Currently the OAIC has undertaken two assessments under this measure and will soon begin its third.

Better privacy practice

- Ensure program protocols include sufficient detail and are up-to-date
- Consider an internal and external version of the protocol to capture sensitive details for corporate knowledge
- Conduct PIAs, and have a system for ensuring any recommendations are implemented
- Use high quality information that is up-to-date, accurate, complete, and fit for purpose
- Actively monitor changing data practices within your agency

Other considerations

- Notifiable Data Breach Scheme
  - Be aware of obligations under the scheme, and consider a Data Breach Response Plan
- Australian Government Agencies Privacy Code (commences 1 July 2018):
  - The Code requires agencies to undertake a written Privacy Impact Assessment (PIA) for all ‘high privacy risk’ projects or initiatives that involve new or changed ways of handling personal information as well as keep a register of all PIAs conducted and publish this register, or a version of the register, on their websites

Questions?

Protecting information rights – advancing information policy

www.oaic.gov.au