"Commercialising and Licensing Anonymised Meta-Data from Personal Information"

Presented by

Tom Meagher
Director

Tom Meagher | Director

Tom has over 30 years' legal and business experience including:

- ✓ being the majority owner and executive director of his former mid-tier Law firm;

- ✓ working for local and major national Law Firms;

- ✓ being a National Operations Manager for a financial advisory IT platform provider

- ✓ being the WA Legal Technology Group Manager for a National Law Firm

- ✓ qualified as a Microsoft-certified Project Manager;

- ✓ owning and managing an IT Consultancy Business; and

- ✓ being a Director and In-House Counsel for a Public Company.

Tom is also a regular publisher of articles and is one of Australia's leading presenters of legal seminars to and for various professional bodies, associations and government authorities on a wide range of business law and professional development-training topics including:

WA Department of Commerce	Institute of Public Accountants	CPA Australia
Chartered Accountants Australia & NZ (CAANZ)	Governance Institute of Australia	Mortgage & Finance Association of Australia (MFAA)
Law Society of WA	National Electrical & Communications Assoc (WA)	City Insolvency Discussion Group
Innovation Centre of WA	Australian Hotels Association (WA)	Forum for Directors of Indigenous Organisations (FDIO)
LegalWise CLE	Small Business Development Corporation	Australian Computer Society
The Tax Institute	Australian Institute of Conveyancers (WA)	Institute of Certified Bookkeepers
Western Suburbs Business Association	Business Foundations Inc	WA Business Assist
WA Reckon Partners	WA Indian Docs Inc.	Australian Institute of Business Brokers (AIBB)

Disclaimer

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

The contents of this presentation are for general information only and intended only as a guide. It does not constitute legal advice and must not be relied upon as such.

Balfour Meagher expressly disclaims all liability for any loss or damage arising from reliance upon any information in this presentation.

If you have a matter that relates to this presentation topic or you require legal advice, careful review and analysis of your matter's particular facts, information and documents are required before proper legal advice can be given or applied to your matter.

What we'll cover

1) What is metadata, open data and personal information?

2) Creative commons licences for research meta

3) What are the current laws in relation to metadata in Australia?

4) Personal information versus other types of proprietary and confidential information

5) Interplay with privacy policies and informed consent

6) Anonymising and de-identifying personal information

7) Relational databases and primary IDs

8) Metadata audience/customers may differ from core business

9) Different metadata having different licensing needs

10) General forms and approaches for metadata licensing arrangements.

1. What is metadata, open data and personal information?

- "**Data**" refers to information. A piece of data could be a line of text, an image or a list of figures.

- "**Metadata**", therefore, is information about data. Metadata provides an explanation or description of the data, which is useful for finding, using and understanding of the information.

  - 'Business metadata is data that adds business context to other data. It provides information authored by business people and/or used by business people.

  - It is in contrast to technical metadata, which is data used in the storage and structure of the data in a database or system.

    – As a simple example, consider a picture of an employee.

      - The picture shows you what that person looks like, but doesn't give any context, such as when the picture was taken, where it was taken, and what role the employee has within the company. Metadata describes the picture, and also provides the additional, unseen information.

- ❖ Put another way – Data is *content*, and Metadata is *context*.

- "**Open data**" is data that can be *freely* used, re-used and redistributed by anyone - subject only, at most, to the requirement to attribute and sharealike*.

- "**Personal data**" may be defined as things such as information about a person e.g. their name, address email, phone number, medical information, date of birth driver's licence passport tax file number etc

- "**Personal information**" is information or an opinion about an identified individual, or an individual who is reasonably identifiable: whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.**

- *source: Open Knowledge Foundation (https://okfn.org/)
- ** Privacy Act 1988 (Cth)
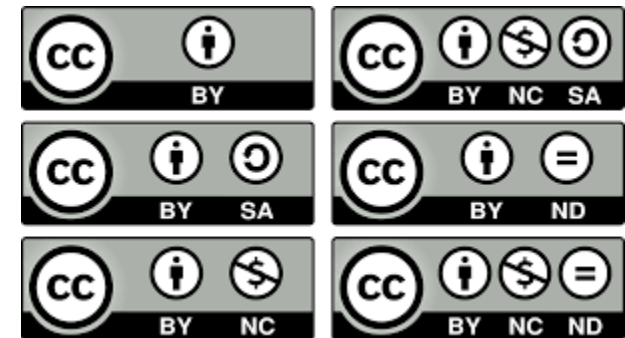
2. Creative commons licences for research metadata

- Creative Commons (www.creativecommons.org) is a global, non-profit organization that enables sharing and reuse of creativity and knowledge through the provision of free legal tools.

- Creative Commons licenses provide an easy way to manage the copyright terms that attach automatically to all creative material under copyright.

- CC licenses allow that material to be shared and reused under terms that are flexible and legally sound. Creative Commons offers a core suite of six copyright licenses.

- As there is no single "Creative Commons license," it is important to identify which of the six licenses you are applying to your material, which of the six licenses has been applied to material that you intend to use, and in both cases the specific version.

- All CC licenses require that users provide attribution (BY) to the creator when the material is used and shared.

- Some licensors choose the BY license, which requires attribution to the creator as the only condition to reuse of the material.

- The other five licenses combine BY with one or more of three additional license elements:

  a) NonCommercial (NC), which prohibits commercial use of the material;

  b) NoDerivatives (ND), which prohibits the sharing of adaptations of the material; and

  c) ShareAlike (SA), which requires adaptations of the material be released under the same license.

- There are 7 licences for which the details are given in the table below (inspired by Foter, 2015):

2. Creative commons licences for research metadata cont'd

Creative Commons Licenses explained, at a glance.

- ✓ (yellow) You can redistribute (copy, publish, display, communicate, etc.) the works.
- ✓ (orange) You have to attribute the original work (title of work, creators name, link, CC license).
- ✓ (red) You can use the work commercially.
- ✓ (green) You can modify and adapt the original work. Provided you indicate how you changed it.
- ✓ (blue) You can choose any license for your adaptations of the work.
- * Intellectual property rights have expired, have been forfeited, or are inapplicable (e.g. works of Shakespeare, Beethoven, etc.)

Disclaimer: This document by its nature cannot be comprehensive and is provided to assist clients to clarify and identify legal issues on which they should seek legal advice. Please consult professional legal staff for advice specific to your situation.

	COPY & PUBLISH	ATTRIBUTION REQUIRED	COMMERCIAL USE	MODIFY & ADAPT	CHANGE LICENSE
COPYRIGHT	✗	✗	✗	✗	✗
PUBLIC DOMAIN*	✓	✗	✓	✓	✓
CC BY	✓	✓	✓	✓	✓
CC BY-SA	✓	✓	✓	✓	✗
CC BY-ND	✓	✓	✓	✗	✓
CC BY-NC	✓	✓	✗	✓	✓
CC BY-NC-SA	✓	✓	✗	✓	✗
CC BY-NC-ND	✓	✓	✗	✗	✓

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

## 2. Creative commons licences for research metadata cont'd

Note: *a CC licence cannot be revoked once it has been issued*.

- CC licenses may be applied to any type of work, including educational resources, music, photographs, databases, government and public sector information, and many other types of material.

- The only categories of works for which CC does not recommend its licenses are computer software and hardware.

- You should also not apply Creative Commons licenses to works that are no longer protected by copyright or are otherwise in the public domain. Instead, for those works in the worldwide public domain, it's recommend that you mark them with the Public Domain Mark.

2. Creative commons licences for research metadata cont'd

❑ Although many scientific data repositories live behind firewalls in proprietary environments, the internet houses thousands of scientific data repositories whose study are now possible.

❑ The Registry of Research Data Repositories by www.re3data.org (a service of DataCite) makes its data available for research under an application programming interface (API). The Registry, now "the largest and most comprehensive registry of data repositories available on the web" publishes an overview of existing international repositories for research data from all academic disciplines and as of September 2016, listed 1692 data repositories.

- **ANDS**: The Australian National Data Service manages Research Data Australia (RDA), a national research data registry. RDA receives contributions from more than 100 Australian research institutions, data infrastructures, and research organisations

- **CERN**: The European Organization for Nuclear Research has different platforms and services related to scholarly information. CERN offers numerous platforms and services related to scholarly information.

- **NCI**: The National Computational Infrastructure (NCI) at the Australian National University (ANU) has evolved to become Australia's peak computing centre for national computational and Data-intensive Earth system science.
  – More recently NCI collocated 10 Petabytes of 34 major national and international environmental, climate, earth system, geophysics and astronomy data collections to create the National Environmental Research Interoperability Data Platform (NERDIP)

- **OpenAIRE**: The OpenAIRE12 infrastructure is the point of reference for Open Access and Open Science in Europe.

- **Research Graph**: This is an example of value added to data infrastructures by third-party services. Research Graph is a collaborative project by a number of international partners that links research information (datasets, grants, publications and researchers) across multiple platforms.

  – This initiative uses the research metadata to construct a graph of scholarly works, and this graph connects data and publications with multiple degrees of separation.

  – The outcome enables a researcher to search the graph for a particular publication or research project and discovers a collaboration network of researchers who are connected to this work (or topic).
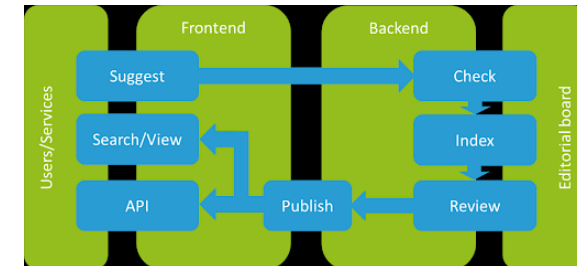
3. What are the current laws in relation to (meta)data in Australia?

➢ In addition to the Privacy Act's relevant provisions relating to a person's (ostensible) metadata such as: sensitive information, health information, credit information, employee record and tax file number information,In 2015, the Australian government introduced mandatory data retention laws that allows data to be retained up to two years. The scheme is estimated to cost at least AU$400 million per year to implement, working out to at least $16 per user per year.

– *The Telecommunications (Interception and Access) Act 1979* (Cth) (the Assistance and Access Act) requires telecommunications companies to retain a particular set of telecommunications data for at least 2 years.

– These obligations ensure Australia's law enforcement and security agencies are lawfully able to access data, subject to strict controls. Access to data is central to almost all serious criminal and national security investigations.

– Australian telecommunications companies will be required by law to retain six different types of metadata from their customers' usage and the information subject to the scrutiny of law enforcement and national security bodies.

• The Assistance and Access Act introduced some key reforms to help our agencies access the evidence and intelligence they need by:
– enhancing industry cooperation with law enforcement and security agencies
– improving agency computer access powers.

• Importantly, nothing in this legislation can require industry to break encryption. Instead, the measures enhance the existing ability of Australian agencies to undertake targeted, proportionate and independently oversighted surveillance activities.

• The Department of Home Affairs' report reveals that law enforcement agencies sought access to information covered by Australia's data retention regime on more than 296,000 occasions in FY18.

- The areas of data to be stored and provided to the government include:

  ❑ Any identifying information linked to the subscribers of accounts with service providers, meaning the names, addresses, phone numbers, email addresses and IP addresses of individuals in accordance with billing details that telecommunications companies have.

  ❑ The source of any communications, meaning the phone numbers, usernames, email addresses and IP addresses of any individual or account that establishes a phone call, SMS message, voice message or email.

  ❑ The destination of any communications. This includes the phone number, usernames, email addresses and IP addresses of any individual who receives SMS messages, voice messages, multimedia communications or emails. This excludes individual's internet browsing histories.

  ❑ The date, time and duration of communication or any details identifying a connection to an internet service (such as Wi-Fi or ADSL).

  ❑ The types of communications and internet services used. This will mean the government will be able to know if individuals send SMS messages, emails, voice messages, chat or forum messages or any social media usage via services such as Wi-Fi or ADSL connections.

  ❑ The physical location from which a communication is made, whether that be the geographic location of a mobile device or the physical address linked to a fixed internet connection.

4. Personal, versus other types of Proprietary & Confidential, Information

- Personal information is different to *proprietary information*, which again may not relate to an individual and therefore would not be subject to privacy laws.

- However various proprietary information, which may not be the subject of statutory *intellectual property* protection such as:
  - patents,
  - trademarks,
  - copyright,
  - designs,
  - circuit board layouts,
  - plant breeder's rights,

  may be valuable and important information that still needs to be protected.

- Commonly any such unregistered or unregistrable proprietary information (which may not have the same protections of intellectual property rights and registrations) can be somewhat protected in other ways.

- **Confidential Information** – the term speaks for itself. But the legalities as to what you can, and cannot, prevent disclosure of, can be complex. Types of confidential information can be business information such as financial records marketing plans customer lists, database.

  - In Australia there is no proprietary interest in confidential information (see cases such as *Pancontinental Mining Limited v The Commissioner of Stamps (1988) 15 IPR 612*). This is in contrast to certain States in the USA where decisions have held that confidential information is property (see, for example, *Carpenter v United States 484 US 19 (1987)).*

  - In Australia, as information is treated as non–proprietary, it is important that contractual terms to deal with the information on the basis of a grant of a right to use or disclose, rather than in terms of an assignment.

  - If a contract is dealing with international rights relating to the confidential information, particularly where US confidential information is involved, it will be necessary to deal with the contractual transmission of those rights on both an assignment and right to use basis.

  - In an action for breach of confidence, the purported confidential information must be identifiable, have some form of originality and not import public knowledge.

4.1 Know How and Trade Secrets

- **Know-how** – this is a collection of different elements that help make your business concept unique.

    - It is the product or service that your business offers, and that others do not (e.g. proprietary procedures and operations manuals, induction and training videos)

- **Trade secrets** - there is no strict legal definition for trade secrets. Instead, the term generally refers to category of information relating to a subject matter of commercial value e.g. all types of technical information.

    - Again, this relates to information of specificity in order to have the necessary quality of confidence. Typical examples of trade secrets may include processes, designs, customer lists, commercial secrets and know-how.

5. Interplay with Privacy Policies and Informed Consent

- Under the Privacy Act, in many cases, the collection, use or disclosure of personal information is justified by the individual's consent.

- This is consistent with the "notice and choice" model for privacy regulation i.e we receive notice of the proposed treatment of our information and we have a choice about whether to accept.

- However, **94%** of Australian do <u>not</u> read or privacy policies that apply to them – and that's rational behaviour. As it would take the average person 244 hours per year (six working weeks) to read or privacy policies that apply to them!*

- Therefore, in many cases, consumers are not truly providing their "informed consent" to current uses of their personal information.

- In fact, the CPRC Report states around one in five Australians: "…*wrongly believed that if a company had a Privacy Policy, it meant they would not share information with other websites or companies*".

 *Consumer Policy Research Centre (www.cprc.org.au - April 2018

5.1 Recent Matter re-: Informed consent lack of transparency & disclosure

- Consider HealthEngine (medical appointments booking app) is now facing multi-million-dollar fines for selling patient data; concerningly including to certain law firms…

    - In August 2019 the ACCC instituted proceedings Federal Court for misleading and deceptive conduct relating to the sharing of consumer information with insurance brokers and the publishing of patient reviews**.

    - "We also allege that patients were misled into thinking their information would stay with HealthEngine but, instead, their information was sold-off to insurance brokers," ACCC chairman Mr Rod Sims said.

    - The ACCC's recent Digital Platforms Inquiry Final Report includes recommendations to strengthen consent and notification requirements under the Privacy Act.

    - "Issues of transparency and adequate disclosure when digital platforms collect and use consumer data is one of the top priorities at the ACCC," ACCC Chair Mr Rod Sims said.

    - "Businesses who are not upfront with how they will use consumer data may risk breaching the Australian Consumer Law and face action from the ACCC." "One of our recommendations from the Digital Platforms Inquiry is that obtaining consent for different purposes of data collection, use or disclosure must not be bundled," Mr Sims said.

    - The ACCC is seeking penalties, declarations, corrective notices and an order for HealthEngine to review its compliance program.

    - The ACCC is also applying for an order from the Court that would require HealthEngine to contact affected consumers and provide details of how they can regain control of their personal information.
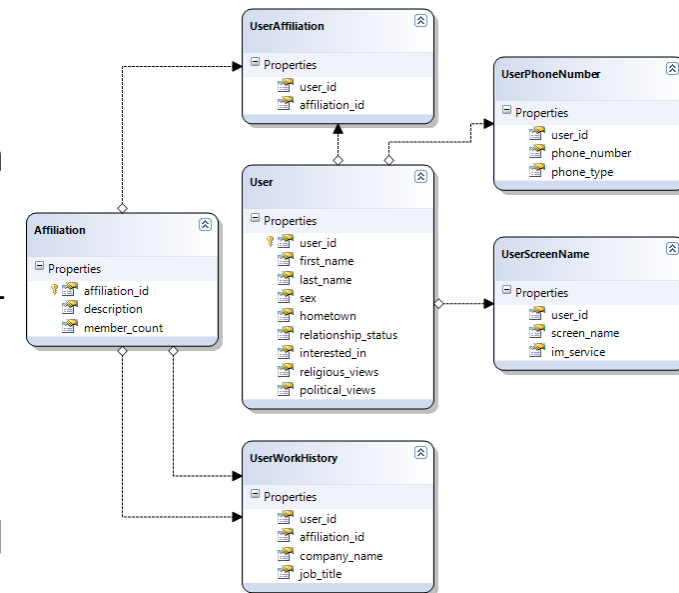
6. Relational databases and Primary Keys

- **What is a relation database ?**

  - A relational database is type of database which uses a set of formally-described tables from which data can be accessed or reassembled in many different ways without having to reorganize the database.

name	age	country
Natalia	11	Iceland
Ned	6	New York
Zenas	14	Ireland
Laura	8	Kenya

6.1 Relational databases cont'd

- Relational Databases use a structure which allows us to identify and access data in relation to another piece of data in the database.

- The standard user and application programming interface (API) of a relational database is the Structured Query Language (SQL).

  - Popular relational database management systems are things such as Oracle DB, SQL Server, and MySQL. These are regularly used by "big data".

  - As small scale RDMS is things such as MS access or FileMaker Pro.

- MS Outlook is a type of database and it actually can be synchronised with any SQL database using open database connectivity (ODBC) support.

6.2 Primary Keys

- **What is the importance of a primary key in a database?**

  – Choosing a primary key is one of the most important steps in good database design.

  – A primary key is a special column (or set of combined columns) in a relational database table, that is *used to uniquely identify each record*.

  – A database primary key cannot contain NULL values and each table can have only one primary key.

  – The values that compose a primary key column are unique i.e no two values are the same.

  – A primary key makes it convenient for a user to add, sort, modify or delete data in a database.

  – Usually integers are the best choice for primary keys because they are fast to create in 'auto increments' and so forth.

Primary Key	Secondary Key		
Roll_No	Name	Branch	City
01	Deepak	Computers	Bhiwani
02	Mukesh	Electronics	Rohtak
03	Teena	Computers	Bhiwani
04	Deepak	Electronics	Rohtak
05	Monika	Computers	Delhi

- In general, if the application containing a database (DB) is designed and secured properly, then revealing meaningless User IDs should not pose a security risk. However, this is not true for all primary key fields in the DB.

- For example, suppose there is an email validation table that has a guide which appears in a link that is emailed to the user. Those single-use IDs should not be made public because otherwise someone would be able to submit a fake email address and still validate it.

- Consider things like your Practice Management System, Outlook , Xero and so forth which has the ability to capture in its huge amount of information relating to anyone, and their various matters it also particular their personal information e.g.

    - Full Name,

    - Address,

    - Mobile Phone Number,

    - Email Address,

    - Residential Address,

    - Credit Card & Banking Information,

    - Date of Birth,

    - Driver's Licence,

    - Passport Number; and

    - possibly even Tax File Numbers.

Examples of Poor Primary Keys

Any field that is missing one or more of the characteristics of a good candidate key is a poor choice for a primary key. Here are a few examples, along with reasons why they would be poor choices.

POOR PRIMARY KEY	REASON
Personal name	Might not be reliably unique, and may change
Phone number	Likely to change.
E-mail address	Likely to change.
Zip code	More than one town may share a ZIP code
Combinations of facts and numbers	Can be hard to maintain, and could lead to confusion if the fact portion is repeated as a separate field. For example, an account ID comprising the city and an incremented number (e.g., NEWYORK0579) would be a poor choice if the city is also stored as a field.
Social Security Numbers	• Private information and not allowed in government departments and some organizations. • Some people don't have a SSN • An individual may have more than one in a lifetime

Access Lesson 2 Lesson Plans
Michele Smith - North Buncombe High School, Weaverville, NC 28787

7. Anonymising and De-identifying Personal Information

- **What is Anonymised data?**

  - Anonymous information means that the data subject is no longer identifiable. The process however must be irreversible*.

- **How can you Anonymise data?**

  - There are different ways of genuinely anonymising data. The two most commonly used are randomisation and generalisation:

  - Randomisation involves the alteration of the data, to remove the link between the individual and the data, without losing the value of the data.

  - Generalisation involves a modification of the level of detail in the data, for example using age ranges from 18-25 rather than a specific age.

Spectrum of identifiability

7.1 De-identifying Personal Information

De-identification and the Privacy Act

- De-identification is a privacy-enhancing tool. When done well, it can help your entity meet its obligations under the Privacy Act and build trust in your data governance practices.

- Information that has undergone an appropriate and robust de-identification process is not personal information and is therefore not subject to the Privacy Act.

- Whether information is personal or de-identified will depend on the context. Information will be de-identified where the risk of an individual being re-identified in the data is very low in the relevant release context (or data access environment).

- Put another way, information will be de-identified where there is no reasonable likelihood of re-identification occurring.

- De-identification involves two steps. The first is the removal of direct identifiers. The second is taking one or both of the following additional steps:
  - ➢ the removal or alteration of other information that could potentially be used to re-identify an individual; and/or
  - ➢ the use of controls and safeguards in the data access environment to prevent re-identification.

- The OAIC recommends that entities also refer to the De-Identification Decision-Making Framework, produced jointly by the OAIC and CSIRO-Data61, which provides a comprehensive framework for approaching de-identification in accordance with the Privacy Act.

7.2 De-identifying Personal Information

Risks with Anonymised data

- Recent research from Belgium's Université catholique de Louvain (UCLouvain) and Imperial College London say it is impossible for researchers to fully protect real identities in datasets.

- The researchers, led by Luc Rocher at UCLouvain, argue their results show that anonymisation is not enough for companies to get around laws such as GDPR (general data protection regulation).

  – "Our results reject the claims that, first, reidentification is not a practical risk and, second, sampling or releasing partial datasets provide plausible deniability.

-

  – "Moving forward, they question whether current deidentification practices satisfy the anonymisation standards of modern data protection laws such as GDPR and CCPA [California Consumer Privacy Act] and emphasise the need to move, from a legal and regulatory perspective, beyond the deidentification release-and-forget model."

- Other approaches for handling large-scale datasets might be more in line with modern data protection needs. Differential privacy, used by companies such as Apple and Uber, deliberately 'fuzzes' every individual data point in a way that averages out across the dataset, preventing deanonymisation by reporting technically incorrect information for each person.

7.2 De-identifying Personal Information

Risks with Anonymised data cont'd

- Researchers were able identify individuals in Medicare data that were supposed to be anonymous, potentially exposing the private information of people receiving mental health treatment or HIV medication.

- Published by the federal Department of Health in August 2016 as part of a move towards open data, the historical information included the medical and pharmaceutical bills of about 10 per cent of Australians.

- It was pulled offline in 2017, after experts from the University of Melbourne were able to decrypt or decode a number of doctor ID numbers.

- In a subsequent report, the Melbourne team describe how they were able to use information easily available on the internet to possibly identify seven famous Australians within the same dataset, without figuring out their patient ID numbers…

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

medicare
1234 56789 1
1 JOHN   A CITIZEN
2 JANE   A CITIZEN
3 JAMES   A CITIZEN
4 JESSICA A CITIZEN
VALID TO 08/2020

7.3 De-identified Public Data

- For public data, the sponsor needs to make a worst-case assumption and protect against an adversary who is targeting the data subjects with the highest risk of re-identification.

- For a non-public data set, we consider three types of attacks:

  1) a deliberate re-identification by the data recipient (or his/her staff and subcontractors);

  2) an inadvertent re-identification by the data recipient (or his/her staff and subcontractors); and

  3) a data breach, where data are accidentally exposed to a broader audience.

- These three cases are relevant when microdata are being disclosed.

- If the data are made available through a portal, we assume that the sponsor will ensure that stringent controls and appropriate auditing are in place, which manages risks from the first and third types of attack. In such a case, the second type of attack, where data may be inadvertently re-identified, becomes the primary risk which needs to be managed.

- An example is if the statistician working with the data inadvertently recognizes someone he or she knows.

Tailored approaches are needed for different types of data

A careful, staged approach to implementation is required to adequately address the different risks, governance requirements and other considerations that each type of data poses.

Type	Example	Access
Personal data	E.g. Individual citizen health records	**Agency access** – for service delivery
Research data	E.g. De-identified, linked health & welfare records	**Restricted sharing** – de-identified data securely shared with trusted users for research
Open data	E.g. Aggregated or non-sensitive data such as Centrelink office locations	**Publicly available** – e.g. through data.gov.au or the ABS Table-builder
Security data	E.g. Metadata collected for intelligence	**Closed access** – not in scope

8. Metadata Audience/Customers may differ from Core Business

- With the traditional or usual target market and customer base of a particular business may not necessarily also be the commercial consumers of that business' metadata.

1. By way of an analogy (of course not endorsing for law firms to sell their metadata), with law firms, their core audience are of course their clients.

   – However all the various metadata they may gather, whether intentionally or by default captured in their respective IT systems, about the ranges of clients (by industry, location, $value, matter types etc), they types work and services they provide, may be may be of particular use in interest to service providers such as:
     - Professional Indemnity insurers such as Law Mutual and Marsh
     - Legal research providers such Reuter Thomsons and Lexis Nexis

2. Agricultural software licensor may have farmers and their accountants as customers, however, if they have been a long period of time, they will have extensive metadata useful for other partiesSuch as:
   – Grain harvest data for parties like CBH
   – Fertiliser uses rates for manufacturers like Incitec Pivot, Wesfarmers, Agrow
   – Haulage rates for livestock and grain transporters

3. A hospital may remove patients' names, addresses and dates of birth from a set of health records in the hope researchers may be able to use the large sets of records to uncover hidden links between conditions.
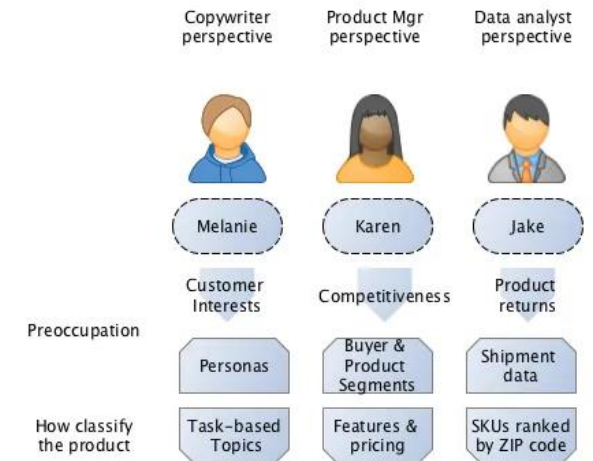
9. General Forms and Approaches for Metadata Licensing Arrangements

IP Master License
1. Definitions and Interpretation
2. Grant of Licence
3. Term and Renewal
4. Licence Fee
5. Licensor's Obligations
6. Licensee's Obligations
   - - exploitation of licence
   - - indemnity and insurance
7. Restrictions
8. Intellectual Property
   - ownership of 'new' Intellectual Property (accretion)
9. Confidentiality and Privacy Undertakings
10. Acknowledgments
11. Default and Termination
    - effects of termination
12. Licensor's Limitation of Liability
13. Continuing Obligations
14. Force Majeure
15. Personal Property Securities Act
16. GST
17. General Provisions

Open Data Licensing Arrangements
- **Publishing your data**
- Publishing open data
- Process to opening a dataset

- **Sourcing data**
- Data from new projects
- Releasing unpublished data

- **Creating datasets**
- Creating a basic open data set:
  - Saved in an open format
  - Data formats
  - Formatted properly for tabular data
  - Formatted to be useful
  - Extra credit

- **Where to publish**

- **Intro to metadata**
- What is metadata?
- How is it used?

- **Licensing your data**

- **Privacy and security**

Proposed Business Structure and Licensing Arrangements
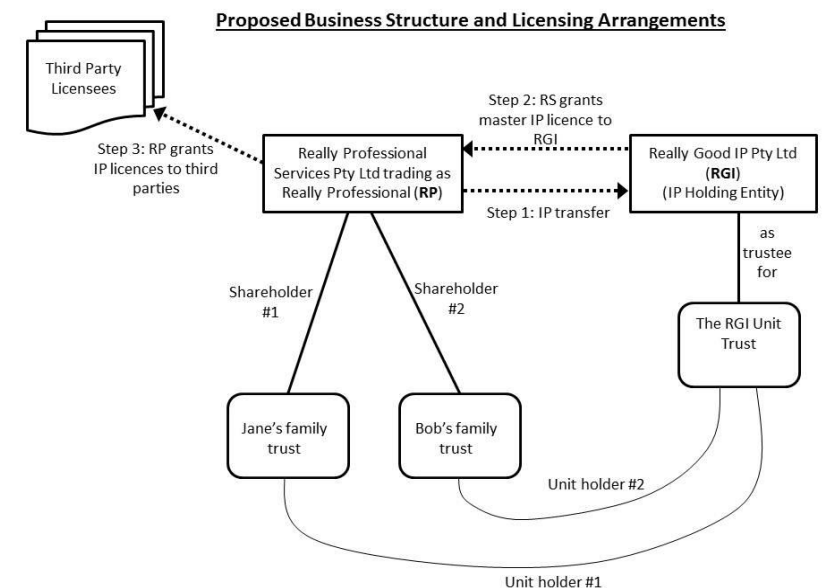
Thank You!

Top-tier quality legal work and business advice delivered directly by highly experienced, personable senior lawyers, business advisors and professional trainers. Balfour Meagher's services include:

- ✓ **Commercial Law**
- ✓ **Technology & Internet Law**
- ✓ **Estate & Business Succession Planning**
- ✓ **Property & Leasing Law**
- ✓ **Property Development**
- ✓ **IP Commercialisation & Brand Protection**
- ✓ **Medical, Pharmacy & Allied Health Services**
- ✓ **Conveyancing and Settlements**

www.bmlegaladvisors.com.au

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

Tom Meagher

Director

E: tom@bmlegaladvisors.com.au

W: www.bmlegaladvisors.com.au

P: +61 8 9322 3842

A: Level 2, 11 Ventnor Ave, West Perth, WA 6005

Email Disclaimer | Subscribe