

A Little Privacy Please

A discussion on Australian Privacy laws in the tertiary education sector

Prepared for SOUL Conference 2024

Prepared by Jennifer Parkes

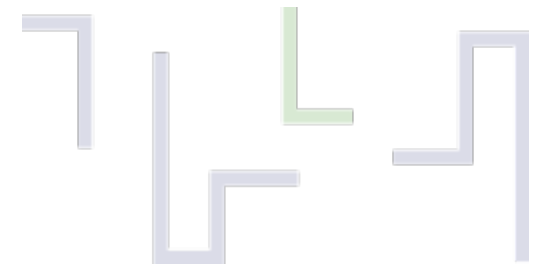
15 November 2024



OVERVIEW



- **Privacy basics**– Australian privacy law principles
- **Legislative developments** – what changes are on the horizon?
- **The state of play in privacy**– risks and current case examples
- **Reflections and recommendations**





WHAT IS PERSONAL INFORMATION?

Personal information

- Information or an opinion about an identified or reasonably identified individual
- part of a database and whether recorded in a material form
- Include genetic and bodily information (retinal scans, for example)

Health information

- Information or opinions about health, illness, disability or injury of an individual
- A person's expressed wishes about providing health services
- Information about the provision of health services

Sensitive information :

- Information or an opinion about:
 - Race and ethnicity
 - Political opinion
 - Religious beliefs
 - Membership of a trade union
 - Sexual orientation
 - Criminal record
- Includes health and personal information



AUSTRALIAN PRIVACY LAWS

For universities:

- If the state or territory has State-based legislation, that **Act** (including if there are separate Acts which manage dealings with personal and health information);
- The Commonwealth *Privacy Act 1998*; and
- The European Union General Data Protection Regulation (**GDPR**), given the likelihood that universities will offer goods and services or monitor the behaviour of individuals in the EU.





AUSTRALIAN PRIVACY LAWS



- **Open and transparent** management
- **Privacy policy**
- **Reasonably necessary collection**
- **Collection notices**
- **Limited use, with consent**
- **Protection** of personal information



COMING UP – LAW REFORM!



Privacy and Other Legislation Amendment Bill 2024

Statutory tort for serious
invasion of privacy

Anti-doxxing measures

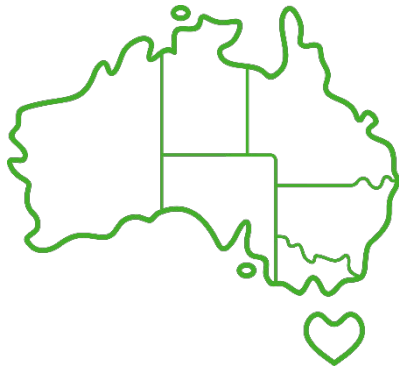
Amendments to APP 11

Amendments *agreed in
principle*

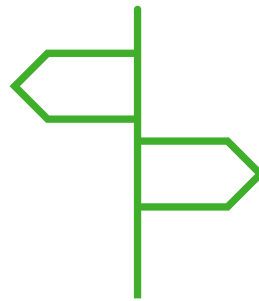


COMING UP – LAW REFORM!

Privacy and Responsible Information Sharing (PRIS) – Western Australia



State-based
scheme, currently
under Federal law



Broad interpretation
of personal
information



Reasonably security
measures for de-
identified information



DO YOU WANT THE BAD NEWS?



- Data breach notifications received by **OAIC** on the increase
- **67%** data breaches from Jan/June 2024 due to malicious/criminal attack (30% due to **human error**)
- Most data breaches reported affect a **single** person, however on average over 60,000 people are affected
- Office of the Victorian Information Commissioner (**OVIC**): audit of privacy and security policies of universities of this state in 2020-2021
- More focus on the threat of cyber, less on **holistic** data and privacy management



STATE OF PLAY: CYBER RISK



- July 2022: **Deakin University** - used a staff member's username and password to access information via a third-party provider.
- August 2022: **University of Western Australia** - unauthorised login activity into the student information management system
- August 2023: **University of Sydney**- third-party data breach
- August 2024: **Western Sydney University** - intrusion into the university's Microsoft Office 365 environment via computer laboratory
- October 2024: **Western Sydney University** - unauthorised access to data from a student management system and other back-end data storage systems



STATE OF PLAY: RECENT CASES



- **Pacific Lutheran College [2023] AICmr 98**
 - unauthorised access by an unidentified third party to the email account of a manager of the school.
 - email account contained approximately 180,000 emails, resulted in the sending of phishing emails to 8,332 contacts of the email account.
 - *Usual* to keep personal information about staff, parent and student stakeholders
- **Datatecks Pty Limited [2023] AICmr 97**
 - extent and type of information held by organisation
- Also, **Australian Clinical Labs Ltd**
 - Proceedings by Privacy Commissioner to prosecute for failing to carry out reasonable investigation of breach



STATE OF PLAY: RECENT CASES



- ***EPT v The Sydney Children's Hospital Network* [2022] NSWCATAD 137**
 - Manager held personal information (including credit card statements and payslips) about an employee on part of the common network drive; without employee's knowledge
 - conceded that certain staff members could search the data base where personal information was stored, in breach of NSW Act
 - that the information was copied for viewing to the unsecured drive was not a breach of use/disclosure principles
 - Suspicion that personal information was being used insufficient to prove breach



STATE OF PLAY: RECENT CASES



- ***Norkin v University of New England* [2023] NSWCA 194**
 - University complied with its obligations, as it was collecting personal information to inquire whether a potential candidate is likely to obtain a student visa, and this was closely related to the function or activity of teaching postgraduate students
 - All purposes for collection of personal information must be identified to understand if there is a direct relationship to the function it intends to put the information collected
 - Meaningfully make the reader aware of the purpose
 - Generic statement that identifies the entirety of the University's functions and activities might not be sufficient



STATE OF PLAY: RECENT CASES



- ***Kerig v Victoria University (Human Rights) [2021] VCAT 532***
 - Employee saved personal and health information to work computer, more than what would be allowed under University policy.
 - The information was discovered by another colleague working on same computer, who complained of the sexual nature of the material
 - Health Records Act (Vic): possession of information, without knowledge, nevertheless under the control of the University
 - Merely locating personal information, without the University's knowledge, **not** collection; discovery of information coincidentally, **not** use or disclosure



KEEP AHEAD OF THE CURVE



Raise awareness of responsibilities



Staff training



Shared accountability



Audit of data storage



Regular review existing collection notices, consents and policies



Meaningful audit of past data breaches

This was a presentation by Jennifer Parkes of Hicksons.

If you require any further information, please contact:



Jennifer Parkes, Partner

T +61 2 4907 5602

E jennifer.parkes@hicksons.com.au

SYDNEY NEWCASTLE

www.hicksons.com.au ABN 58 215 418 381

Liability limited by a Scheme approved under Professional Standards Legislation