Privacy Update

Presented by Francisca Mayer, Associate

VOCARE
LAW

Introduction

CORNEY & LIND
LAWYERS

→

VOCARE
LAW

A little about us...

Same

- Same team, same mission
- Still called to deliver Just, Redemptive Outcomes®
- General practice of law with a particular focus on not-for-profit & charity law.

Different:

- Name change - Vocare (pronounced vo-ka-ray); latin meaning "to be Called.
- Additional **new** office in North Ryde, Sydney.

Today

1. *How would the recommendations under the Privacy Act Review Report affect schools?*

2. *Updates in the Privacy Law and Cyber-security space, including recent cases.*

3. *What are the Office of the Australian Information Commissioner's expectations in taking steps as are reasonable in the circumstances to protect information from unauthorised access (Australian Privacy Principle 11.1(b))?*

4. *What do we think data governance will look like in 2024?*

5. *What are the privacy considerations for use of Open AI and Chat GPT in the classroom?"*

Privacy Act 1988 Framework

VOCARE LAW

Privacy Act Framework

- *Privacy Act 1988* (Cth) regulates how entities can handle personal information.
- Small business exemption ($3M annual turnover) – **but** organisations such as private schools that provide a **health service** (inc. mental health services such as counselling) are covered by the Act

Rights and Remedies

- The *Privacy Act* doesn't give individuals a personal right of action – enforcement is through complaints to the OAIC
- Enforcement model is largely **co-operative**, but OAIC may pursue civil penalties for serious breaches in the Federal Court
  - These are effectively fines, and are **not** paid to the individual.
- **Notifiable data breaches scheme** requires entities to report certain data breaches to OAIC and affected individuals

2022 Amendments

- Significant increase in maximum penalties for serious or repeated breaches of privacy:
  - Individuals: $444K → $2.22M
  - Corporations: $2.5M → higher of: $2.5M, 3x the value of any benefit obtained from the privacy breach, or 30% of adjusted turnover during the period of the breach.
- Enhanced investigative powers for OAIC

The *Privacy Act* Review and Schools

VOCARE LAW

Review of the Privacy Act

- Anticipated legislative changes arising from the Privacy Act Review Report 2022
- 116 proposals were made to amend the Privacy Act 1988 (Cth). In response to the Report the Government **agreed to 38** of the recommendations and **68 of the recommendations were 'agreed in principle'**.
- In light of the recommendations and proposed amendments, organisations are encouraged to consider the reforms immediately in the context of their business and identify whether any amendments need to be made to ensure compliance with the 'agreed' principles.
- With respect to the 68 reforms which are agreed 'in principle' organisations should work towards compliance using lessons learned from global best practice.

Consent & Use - Current

Consent:

- Only necessary for collection of ‘sensitive information’ (e.g. health or biometric information, or information about race, political opinions or affiliations, religion, sexuality, criminal record)
- Consent means “express consent or implied consent”
- No provision for consent to be **withdrawn**

Use:

- Organisations must not collect personal information unless it is reasonably necessary for one or more of their functions or activities (APP 3)

Consent & Use – Proposals

Consent:

- 11.1 – Consent must be “voluntary, informed, current, specific, and unambiguous”
- 11.3 – Consent must be able to be subsequently *withdrawn* (but not so as to affect the lawfulness of any use made of information prior to the withdrawal).

Use:

- 12 – Collection, use and disclosure of personal information must be “fair and reasonable in the circumstances”, *regardless* of whether consent has been obtained.

Protections for Children

- Currently, no bespoke regime for dealing with the personal or sensitive information of children; or for obtaining consent from minors
- Act does not require that consent be given with capacity

Proposal 16

- Child defined to mean under 18; but children can have capacity if of sufficient maturity
  - Rebuttable presumption that anyone over 15 has capacity – operates if impractical to determine capacity on a case-by-case basis
- Consent of the child (with capacity) must usually be obtained when dealing with their data (or consent of a parent/guardian)
  - Exception where involvement of parent or guardian could be harmful to the child or contrary to their interests – e.g. advice/assistance with DV, confidential healthcare, mental health, or drugs

Proposal 16 cont'd

- Entities must consider the best interests of the child when dealing with their data
- Higher bar in terms of clarity for notices and privacy policies addressed to children
- Prohibition on targeting and direct marketing to children except where in child's best interests

Organisational Accountability - Current

- Small business exemption
- APP 1.2 – Entities must take reasonable steps to implement practices, procedures and systems that ensure that the entity complies with the Australian Privacy Principles
- APP 1.3 – Must have a privacy policy that is clear, comprehensive, up-to-date, and accessible
- APP 5.1 – Must notify individuals when their personal information is collected

Accountability – Proposals

- 6.1 – Removal of small business exemption
- 15.1 – purposes for which personal information is collected, used, and disclosed must be determined *at or before* collection, and records made of any additional purposes for which the data was used or disclosed.
- 15.2 – Organisations must designate a specific senior employee to oversee privacy

Individual Rights – Proposal 18

- Act already provides a right to access personal information about oneself held by an entity. Expand to include (upon request) an explanation of:
  - The source of the information
  - A summary of what has been done with it
- Introduce right to request erasing of such information, which request must be communicated to any third parties to whom the information has been disclosed
- Introduce duty on entities to provide ‘reasonable assistance’ to assist in the exercise of rights

Enforcement – Proposals 25-28

Additional emphasis on individual rights, including –

- 25 – New civil penalty provisions for breaches of the Act
- 26 – Direct right of action allowing individuals to sue entities for interference with privacy
- 27 – Statutory tort for serious invasions of privacy
- 28 – Enhancement of the notifiable data breaches scheme

Case Example

VOCARE
LAW

Pacific Lutheran College (Privacy) [2023] AICmr 98

- Staff member's email account was hacked; phishing emails were sent to 8,332 contacts of the account
- PLC quickly become aware of the breach, and that sensitive information was likely at risk (held financial details, tax file numbers, identity information and contact information). All staff were notified the next day
- PLC engaged an independent investigator, investigation progressed slowly over several months
- PLC notified the OAIC six months later

Pacific Lutheran College cont'd

- *Privacy Act* requires an entity who has reasonable grounds to ***suspect*** an "eligible data breach" has occurred:
  - Must carry out an assessment of the breach
  - Must take all reasonable steps to ensure the assessment is completed within 30 days
- If assessment reveals reasonable grounds to ***believe*** an "eligible data breach" has occurred:
  - Report to OAIC as soon as practicable.

Pacific Lutheran College cont'd

- OAIC held that PLC failed to:
  - Conduct an assessment of a data breach in an expeditious manner
  - Notify the OAIC as soon as reasonably practicable
  - Take reasonable steps to protect the affected individuals' personal information from unauthorized use or disclosure
  - Have proper procedures in place for dealing with breaches
- Consequences:
  - PLC declared to be in breach of its obligations
  - PLC ordered to prepare incident response plan and information security program
  - PLC to engage expert to review these and report to OAIC to confirm compliance

Pacific Lutheran College cont'd

- What is considered as a notifiable data breach?
  - unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds
  - this is likely to result in **serious harm** to one or more individuals, and
  - the organisation or agency hasn't been able to prevent the likely risk of serious harm with remedial action.
- If you suspect an eligible or notifiable data breach has occurred, quickly assess the incident to determine if it is likely that serious harm has resulted to an individual.

Pacific Lutheran College cont'd

- What is serious harm?
  - There is no test for what is considered serious harm
  - Objective test from the perspective of a reasonable person
- Considerations
  - Circumstances of the breach
    - Whose personal information was involved
    - How many individuals personal information has been leaked
    - How long was the personal information accessible
    - Who has gained unauthorized access to personal information

Pacific Lutheran College cont'd

- Nature of the Harm
  - Identity theft
  - If there is any financial loss by the individuals
  - Has the individual's physical safety been threatened
  - Has the individual had loss of business or employment opportunities
  - Humiliation or damage to reputation
  - Has the breach caused workplace or social bullying or marginalisation

Reasonable Steps to Prevent Unauthorised Access

VOCARE
LAW

APP 11.1(b)

*11.1 If an APP entity holds personal information, the entity must take **such steps as are reasonable** in the circumstances to protect the information:*

*(a) from misuse, **interference** and loss; and*

*(b) from **unauthorised access**, modification or disclosure.*

- What constitute **reasonable steps** to prevent unauthorized access?

‘Reasonable’

- What is ‘reasonable’ depends on –
  - Nature of the entity – size, resources, complexity of operations
  - Amount and sensitivity of information held
  - Potential consequences for the individual if their data was accessed
  - Time and cost involved in taking remedial action – but mere inconvenience is not sufficient to justify failure to take action, burden must be **excessive**

‘Reasonable steps’

- Reasonable steps generally include –
  - Implementing an overarching protocol dealing with data collection, retention, and destruction
  - Training for staff that focuses on data protection
  - Ensuring adequate ICT security and access protocols
  - Developing a plan for preventing and responding to data breaches (hacking)
  - Ensuring data is kept no longer than necessary

Data Retention – APP 11.2

- Don’t retain information longer than necessary - must destroy or de-identify information if no longer required by the organization or by law
  - Personal information is destroyed when it can **no longer be retrieved**
  - If de-identifying, assess the risk of re-identification – this is often easier than imagined!
  - If data is stored with a third party, take steps to ensure instruction to destroy data has been adequately implemented
- Implement policies to **actively consider** whether information is still required

AI in Schools: Privacy Considerations

VOCARE
LAW

ChatGPT – Risks

- Entering sensitive information
- Entering information from which sensitive information can be deduced
  - Conversational AI naturally invite disclosure of much more personal information than traditional search engines
  - AI can and does build a comprehensive picture of users, and accurately infers sensitive information from seemingly innocuous input
- Hacking

ChatGPT – Disclosure

- OpenAI's *Privacy Policy* states:

  In certain circumstances we may provide your Personal Information to third parties without further notice to you, unless required by the law:

  Vendors and Service Providers: To assist us in meeting business operations needs and to perform certain services and functions, we may provide Personal Information to vendors and service providers, including providers of hosting services, customer service vendors, cloud services, email communication software, web analytics services, and other information technology providers, among others. Pursuant to our instructions, these parties will access, process, or store Personal Information only in the course of performing their duties to us. …

ChatGPT – Risk Management

- Many prominent companies are banning ChatGPT because the risks of disclosure of sensitive information are too great – e.g. Apple, Samsung, Goldman Sachs, JP Morgan, Citigroup
- Using ChatGPT in schools is never risk-free, but risk can be managed through implementing comprehensive protocols and proper education of teachers and students.

ChatGPT – Legal Issues

- Intellectual Property and Ownership Issues
  - Legal ownership of the content created. Is the teacher and/or educational institution the proprietor, or is it ChatGPT?
  - Recently, the Australia Federal Court in *Thaler v Commissioner of Patents* [2021], found that AI could not be credited as being an 'inventor' of a patent under the Patents Act, as it is not a natural person, and therefore incapable of owning intellectual property.
  - Whilst the Thaler case provides a useful illustration of this constantly evolving technological space, it leaves many questions unanswered.

- As a starting point, sub-clause 3(a) of OpenAI's (the creator of ChatGPT)

ChatGPT – Legal Issues

- Intellectual Property and Ownership Issues
  - As a starting point, sub-clause 3(a) of OpenAI's (the creator of ChatGPT) Terms of Use Policy purports:
    - As between the parties and to the extent permitted by applicable law, you own all Input. Subject to your compliance with these Terms, OpenAI hereby assigns to you all its right, title and interest in and to Output. This means you can use Content for any purpose, including commercial purposes such as sale or publication, if you comply with these Terms.

ChatGPT – Legal Issues

Intellectual Property and Ownership Issues

- While OpenAI does not use data submitted by customers to their API3 to develop or improve Services, the same cannot be said for ChatGPT. When users engage with ChatGPT, OpenAI stipulates at subclause 3(c) of its Terms of Use Policy that it may utilise the content "to help develop and improve our Services".
- What does this mean for educators? By way of example, Teacher A uses the ChatGPT prompt tool to create a lesson plan based on a pre-existing set of learning objectives. Ownership of both the learning objectives and lesson plan generated remains and is assigned respectively to the user, here, the teacher.
- But, the data from both the input (learning objectives) and the output (lesson plan), per clause 3(c) may be used to improve the ChatGPT model. So, if an unrelated Teacher B subsequently requests either a lesson plan or learning objectives, the product generated by ChatGPT to satisfy this request may draw from the information entered and generated by Teacher A.

ChatGPT – Legal Issues

Intellectual Property and Ownership Issues

- While OpenAI does not use data submitted by customers to their API3 to develop or improve Services, the same cannot be said for ChatGPT. When users engage with ChatGPT, OpenAI stipulates at subclause 3(c) of its Terms of Use Policy that it may utilise the content “to help develop and improve our Services”.
- What does this mean for educators? By way of example, Teacher A uses the ChatGPT prompt tool to create a lesson plan based on a pre-existing set of learning objectives. Ownership of both the learning objectives and lesson plan generated remains and is assigned respectively to the user, here, the teacher.
- But, the data from both the input (learning objectives) and the output (lesson plan), per clause 3(c) may be used to improve the ChatGPT model. So, if an unrelated Teacher B subsequently requests either a lesson plan or learning objectives, the product generated by ChatGPT to satisfy this request may draw from the information entered and generated by Teacher A.

ChatGPT – Legal Issues

➢ Copyright

- Input of data to train ChatGPT is problematic.
- The intersection of the Privacy Principles and AI is another area for close consideration.
- Primarily, the Privacy Policy of OpenAI provides for the collection of the following personal information:
  a. account information and user content;
  b. the contents of any messages [users] send (referred to as Communication Information);
  c. Internet Protocol address, browser type and settings, and how users interact with the website; and
  d. the types of content that users view or engage with, the features users utilise and the actions users take, as well as time zone, country, the dates and times of access, user agent and version, type of computer or mobile device, computer connection, IP address and 'the like'.

ChatGPT – Legal Issues

- Hypothetical
  - Teacher asks ChatGPT to provide suggestions regarding a student's individual learning plan. The teacher includes specific information about the student, including their learning difficulties and sensitive personal background.
  - In circumstances where ChatGPT can extract the contents of any message, this would constitute a breach of Privacy Principle 11.1(b), which requires schools to take such steps as are reasonable in the circumstances to protect personal information from unauthorised access, modification or disclosure.

ChatGPT – How can schools manage and mitigate legal risks?

- Schools should implement appropriate policies to provide clarity for its educators.
- If permitting teachers to utilise ChatGPT, teachers should ensure material is cross checked for accuracy prior to use. Furthermore, when using the service to draft policies, procedures and marketing material, the information should be appropriately reviewed and verified.
- n creating new policies and approaches to ChatGPT and similar technologies, schools should consider strategies to integrate these technological tools in the classroom. Since they will remain a fixture within the technological landscape, empowering students to effectively and ethically use these new tools is a productive approach.
- Schools should maintain open communication about steps being taken to manage these challenges. While this will be an ongoing process, schools may need seek external resources and support in educating themselves on policies and procedures that are up to date, comprehensive and legally sound.

ChatGPT – Education

- Teachers –
  - Disclosure of sensitive information about a student to an AI is a breach of confidentiality
  - Safest policy is to avoid telling AI anything about students as AI might infer confidential information
- Students –
  - ChatGPT stores your conversations by default, but you can change the settings
  - AI is not a friend: if you wouldn't tell a stranger on the internet, don't tell ChatGPT
  - ChatGPT can infer sensitive information about you

Questions

VOCARE
LAW

VOCARE

LAW

Thank you.

Francisca Mayer
Associate

fran.mayer@vocarelaw.com.au
1300 862 529
vocarelaw.com.au