Privacy & Data Law

Andrew Hynd

9 May 2023

HOLDING REDLICH

About me

- Andrew Hynd
  - Partner
    - Technology and Innovation
    - Data and Privacy
    - Procurement and Probity
  - 25 years' experience
- Holding Redlich
  - Full service law firm
  - 200 staff in Brisbane
  - Offices in Brisbane, Cairns, Sydney, Melbourne and Canberra

Technology

- “Technology is a useful servant but a dangerous master.” – Christian Lous Lange
- “Once a new technology rolls over you, if you’re not part of the steamroller, you’re part of the road.” – Stewart Brand
- “It’s not that we use technology, we live technology.” – Godfrey Reggio
- “The real problem is not whether machines think but whether men do.” – B.F. Skinner

- “Every business is a technology business” - me
- "Technology is a word that describes something that doesn't work yet." - Douglas Adams

Outline for today

- Cyber Security – what is it and how prevalent?
- Identification of risk and regulatory environment
- Recent cases
- Privacy Act review
- Chat GPT
- SOCI Act
- Risk management

Cyber Security – what is it and how prevalent?

- Cyber Security
  - practice of defending computers, servers, devices, electronic systems, networks and data from unauthorised access, use, disclosure, disruption, modification, destruction, or malicious attack
  - not necessarily a data breach for privacy law purposes, unless “personal information” involved

- Threats
  - business email compromise
  - malware/ransomware
  - hacks into systems and cloud

- Organisations must be alert
  - hackers are constantly seeking to exploit security weaknesses

- Be prepared to be the target of an attack
  - proactive not reactive

Identification of risk and regulatory environment

- Operational issues, including:
  - staff may not be adequately trained to identify cyber security threats
  - organisation may not have a comprehensive list of its IT systems nor any classification of IT systems based on importance
  - third party suppliers are increasingly the weak link, and supply chain merits analysis and rigorous practices

- Consider the regulatory environment and particular obligations on the organisation, and whether it is in a sector that is targeted, or will constitute “critical infrastructure”

Recent cases and responses to them

a) Optus, Medibank Private and others
b) RI Advice
c) New penalties
d) Privacy Act review
e) Facial recognition investigations and proposals

How bad can it be?

- Consider Maersk NotPetya incident
- Russian cyber attack on Ukraine
- Spread through 60 countries
- Maersk heavily affected
  - All 1,200 applications inaccessible
  - Fixed line phones didn’t work
  - Mobile contacts wiped
  - Rebuild of entire network

OAIC Report July to December 2022

- 497 notifications (up 26%)
- Health still top sector, followed by finance and insurance
- 70% malicious attacks (41% increase)
- 45% result from cyber security incidents – breakdown:
  - 29% ransomware
  - 27% compromised or stolen credentials
  - 23% phishing
- 88% contact information, 60% identity information
- 71% notified OAIC within 30 days

What do people want?

- Privacy is a major concern for 70%
- Nearly 90% want more choice and control over personal information
- Data privacy more important than reliability, convenience and price
- >50% had a problem with use of data in last 12 months:
  - Unwanted marketing communications
  - Unnecessary collection of personal information
- 66% backed out of purchase/closed account due to privacy concerns

The current landscape

Qld public sector

Information Privacy Act 2009 (Qld)

Information Privacy Principles

National Privacy Principles (Queensland Health)

Cth public sector

Privacy Act 1988 (Cth)

Information Privacy Principles

Private sector

National Privacy Principles

Australian Privacy Principles

Global

GDPR

Privacy Act review

- “Organisations should take appropriate and proactive steps to protect against and respond to a range of cyber threats,” Commissioner Falk said. “This starts with collecting the minimum amount of personal information required and deleting it when it is no longer needed”
- Key features:
  - Less exemptions
  - Overarching obligation to be fair and reasonable
  - Shorter data breach notification timing
  - Automated decision making
  - Right of erasure
  - Direct right to sue
  - More specific record keeping obligations

Chat GPT

- James Cook University (JCU) in Australia has a well-regarded law program. JCU's Bachelor of Laws (LLB) degree is accredited by the Legal Practitioners Admissions Board, which means that graduates of the program are eligible to apply for admission to legal practice in all Australian states and territories.
- JCU's law program has a strong focus on social justice and practical legal skills. Students are taught by experienced legal practitioners and academics and have access to a range of experiential learning opportunities, including clinical placements and moot court competitions.
- JCU also offers a range of specialized law courses, including courses in environmental law, international law, and Indigenous peoples and the law.
- Overall, JCU's law program is well-regarded and prepares graduates for a range of legal careers.

- GPT Zero: **Your text may include parts written by AI**

Limitations

- Chat GPT
  - The maximum penalty for a serious or repeated breach of privacy under the Australian Privacy Act 1988 (Cth) is **AUD 2.1 million** for corporations. Individuals can also be held personally liable for breaches, and may face fines of up to **AUD 420,000**. These penalties apply to breaches of the Australian Privacy Principles (APPs) that govern the handling of personal information by Australian entities, as well as breaches of the Notifiable Data Breach (NDB) scheme, which requires entities to report certain data breaches to affected individuals and the Office of the Australian Information Commissioner (OAIC). It's important to note that the actual penalties imposed may vary depending on the severity of the breach and other factors considered by the OAIC.

- Current
  - The 'civil penalty provisions' in the Privacy Act include: a serious or repeated interference with privacy (s 13G) with maximum penalties including **$2,500,000** for a person other than a body corporate, and for a body corporate, an amount not exceeding the greater of:
    - **$50,000,000**; or
    - three times the value of the benefit obtained directly or indirectly by the body corporate and any related bodies corporate, that is reasonably attributable to the conduct constituting the contravention; or
    - if the court cannot determine the value of the benefit, 30% of the body corporate's adjusted turnover during the breach turnover period for the contravention.

SOCI Act and critical infrastructure assets

Original scope

Electricity
Ports
Water
Gas

Current scope

Telecommunications, broadcasting, domain name systems, data storage or processing, banking, superannuation, insurance, financial market infrastructure, water, electricity, gas, energy, liquid fuel, hospitals, education, food and groceries, ports, freight infrastructure, freight services, public transport, aviation, defence industry

Key obligations

- Reporting operational and control information
- Compliance with Cth directions + information requests
- Reporting cyber events
- Critical Infrastructure Risk Management Plan/reporting for exempt critical infrastructure assets
- Enhanced cyber security obligations if System of National Significance

How the cyber security notifications obligations work

The Minister specifies what critical infrastructure assets are subject to the security notification obligations following consultation (ss 30BB & 30BBA). Those include a critical infrastructure asset that you are responsible for.

A cyber security incident occurs or is occurring

The incident is of "significant impact"

You must report to Cth ASAP and within 12 hrs

The incident is of "relevant impact"

You must report to Cth ASAP and within 72 hrs

Penalties = $11,100 for individuals and $55,500 for body corporates

Risk Management

- **Setting the scene**
  - Regulator interest and resourcing
  - Higher penalties
  - Reputational consequences

Risk Management (cont)

- Communicate risk information so decision makers can make fully-informed decisions
- Install appropriate security software to prevent hackers gaining access
- Contract review - incident response steps and allocation of responsibility
- Keep your security software and your operating system up to date, ensure backups are regular
- Talk to a suitably qualified IT advisor about cyber security and identify the risks in your systems, including in the architecture to ensure sufficient separation of systems
- Provide cyber security awareness training to all staff, encourage regular discussions

Risk Management (cont)

- Always check the legitimacy of any changes to processes/payment instructions
- Ensure you have strong passwords that satisfy current best practices for length and complexity
- Use multi-factor authentication wherever available
- Have cyber security policy prepared and enforced, and train staff appropriately (not sharing passwords)
- Establish an access control system, restrict administrator privileges
- Create a cybersecurity incident response plan

Risk Management (cont)

- Undertake PIAs ahead of time
- Given 4 of 5 incidents involve user error, focus on training
- Update plans and controls for changes in structure or function
- Check legacy systems
- Consider specific insurance, rather than rely on general policies
- Consider data mapping exercise
- Simulate attacks and test your comms teams

Practical tips for managing a cyber attack

- Communicate with incident response team
  - internal team of decision makers
  - IT team members
  - external cyber consultants and legal advisors
  - potentially may also need PR consultants
- Initial damage limitation
  - is attack ongoing?
  - do systems need to be suspended?
- Breach impact and risk assessment
  - What happened?
  - What data is involved, and where did this originate from?
  - How sensitive was the data?
  - What individuals are involved, how many?
  - What is potential harm?

Practical tips for managing a cyber attack (cont)

- Respond to threats/extortion
  - payment of money?
  - consider how to respond, seek advice where required
- Notification and external considerations
  - manage PR and any external complaints
  - inform various bodies: police, insurance, banks, any individuals involved, contact relevant regulator
- Learnings
  - know the data you hold
  - know where the data is held
  - know who has access to it
  - know who is protecting it and how well

Questions?

Thank you

HOLDING REDLICH


HOLDING REDLICH