Privacy and Sport update

New South Wales Office of Sport

Member Protection in Sport

24 July 2018

Overview – Australian Privacy Law

- *Privacy Act 1988*
  - Public organisation (IPPs)
- *Privacy Amendment (Private Sector) Act 2000*
  - Private organisations (NPPs)
- *Privacy Amendment (Enhancing Privacy Protection) Act 2012*
  - Effective 12 March 2014
  - Unified “Australian Privacy Principles” (APPs)
- *Privacy Amendment (Notifiable Data Breaches) Act 2017*
  - Effective 17 February 2018
- GDPR

LEX SPORTIVA

Privacy Act (Act)

- The Australian Privacy Principles (APPs) in schedule 1 of the Act
- Australian Government agencies, all private sector and not-for-profit organisations with an **annual turnover of more than $3 million**, all private health service providers and some small businesses (collectively called ‘APP entities’) must handle, use and manage personal information
- Act applies to businesses that are incorporated in Australia. It also applies to businesses outside Australia if they collect personal information from, or hold personal information in, Australia and carry on a business in Australia (s 5B of the Act)

LEX SPORTIVA

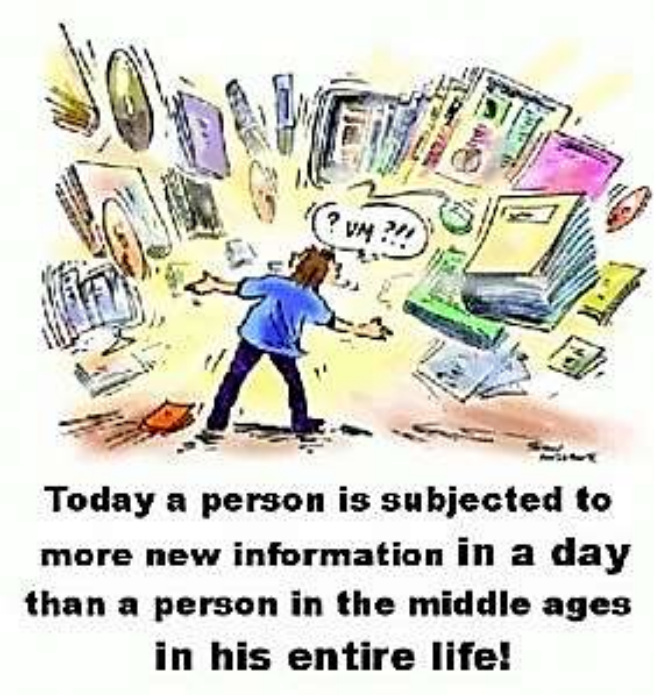
Personal Information

- Section 6(1) Privacy Act 1988
- Personal information:
  - "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."
- Three key parts:
  - Must be a statement of fact or opinion
  - Identity must be included or identifiable
  - Must be in a record

LEX SPORTIVA

Why is protecting privacy important?

- Technology is changing
  - sophisticated, rapid and free flowing sharing of personal information



LEX SPORTIVA

Why is protecting privacy important?

- Commissioner's new powers
- Consumers care about privacy matters
- Reputational damage

LEX SPORTIVA

Case study

- Medvet is an on-line health and safety website
- Media reports claimed that names and addresses of Medvet customers who had ordered paternity or drug & alcohol tests had been made available on the internet.
- The Commissioner opened an Own Motion Investigation…

The Sydney Morning Herald
Technology

Paternity and drug test details leak online in privacy breach

July 18, 2011

Comments 3

Asher Moses

Australians who bought drug and paternity tests from one of the country's largest providers are dealing with a serious privacy scare after details of their orders were found to be available online.

> *"The Medvet messaging has been quite slow and they appeared unconcerned with the matter"*

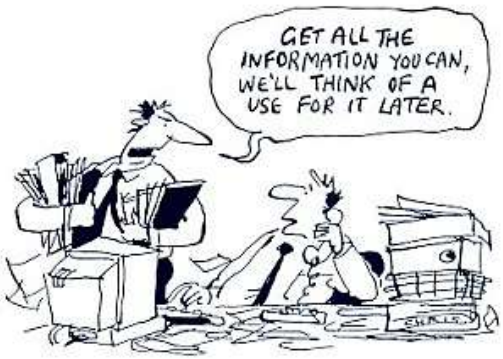
Medvet, owned by the South Australian government, appears to have failed to lock down its online order system and prevent it from being crawled by Google. Hundreds of orders of tests from people all over Australia can be found by searching Google for a specific term, which Fairfax Media has chosen not to publish.

Case study

- The Commissioner made a finding that the accessibility of address information on the internet constituted unlawful disclosure of personal information in contravention of the Act.
- The Commissioner also found that Medvet did not have reasonable steps in place to protect personal information, in contravention of the Act.

Privacy obligations

- Privacy policy
- Collection notices
- Unsolicited information
- Storage & Use
- Sensitive information
- Direct marketing
- Cross-border disclosure



LEX SPORTIVA

Obligations & discussion

- Privacy policy
  - types of personal information collected
  - how the info is collected and used
  - why it is collected, used and disclosed
  - how individuals can access and correct their information
  - complaint procedures
  - list of overseas countries where info may be disclosed
  - Also – new anonymity and pseudonymity requirements

LEX SPORTIVA

Obligations & discussion

- Collection notifications
  - organisation's identity and contact details
  - fact information is being collected
  - whether required or authorised by law
  - purpose/s of collection
  - consequence if not collected
  - information about access and correction & complaints process
  - list overseas countries where likely to be disclosed

LEX SPORTIVA

Obligations & discussion

- Storage & use
  - Most often breached
  - Use - concept of ‘primary’ and ‘secondary’ purpose
  - Can only use information for the ‘primary’ purpose it was collected
  - Can use the information for a ‘secondary’ purpose if an exemption applies: ie, legally required, health situation, court order, etc

LEX SPORTIVA

AAPT Case study

- Internet activists ‘Anonymous’ hacked into AAPT servers and stole 40gb of data
- Files stolen ranged from internal employee data through to customer information
- Stolen info included: individual identity verification details, billing data and credit information & published online
- The Privacy Commissioner got involved…

LEX SPORTIVA

AAPT

b | The ABC interviews Anonymous regarding AAPT hack

BY NICK ROSS AND LISA MAIN

ABC TECHNOLOGY AND GAMES : UPDATED 30 JUL 2012 (FIRST POSTED 26 JUL 2012)

COMMENTS (17)

The hacktivist group Anonymous has given an interview with the ABC with regards to its hacking of an Australian ISP. While details are impossible to 100 per cent verify at present, the sources of this interview are verified as being the sources behind the hacking announcements.

Artist's impression of hackers.

AAPT Case study

- Why is this a Privacy breach?
- Why would AAPT be under the spotlight for being the *victim* of hackers

LEX SPORTIVA

AAPT

AAPT Case study

- Commissioner investigated (OMI).
- Found that AAPT:
  - failed to comply with its obligation to destroy or permanently de-identify information no longer in use;
  - failed to have contractual measures in place with the third party responsible for its servers;
  - failed to adequately protect the security of its customers' information; and
  - failed to take steps of its own to update relevant software.

LEX SPORTIVA

AAPT

Case study

- Complaint to Commissioner by an individual
  - The individual complained to the ombudsman that she had concerns regarding her employer (JACS) breaching public safety matters involving minors and liquor
  - The regulator called the employer (JACS) regarding the complaints in order to determine if the concern was frivolous or vexatious
- When contacted, staff of the employer advised that:
  - The individual had personal problems
  - Worked as a bookie & involved in other illegal matters

LEX SPORTIVA

ACT Government
Justice and Community Safety

Case study

- Individual complained to Privacy Commissioner that her former employer (JACS) had no right to disclose that information.
- Did it?

Case study

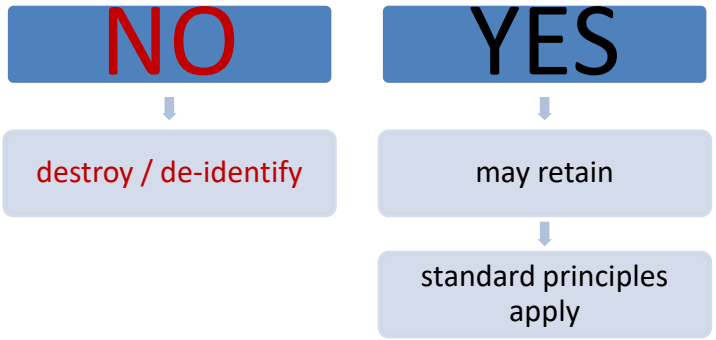
- Answer – no
  - Commissioner found that it was not relevant to whether the Complainant's disclosure was frivolous or vexatious for JACS staff to disclose detailed personal information about the Complainant's background and work matters
  - Privacy obligations cover internal & external information
  - Need for staff training & awareness
  - Need for policy and procedures put in place

LEX SPORTIVA

ACT Government
Justice and Community Safety

Unsolicited information

- Ask yourself: "is this information reasonably necessary for one or more of my business' functions or activities?“



LEX SPORTIVA

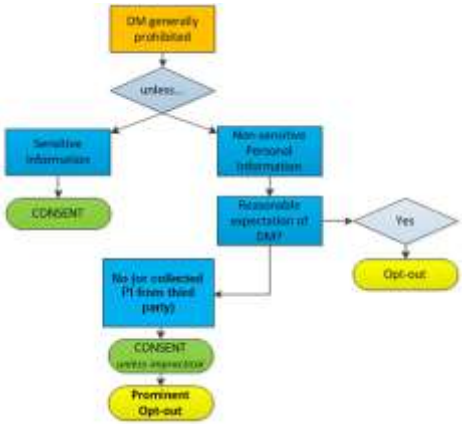
Sensitive information

- Information or an opinion about an individual's:
  - racial or ethnic origin; or
  - political opinions; or
  - membership of a political association; or
  - religious beliefs or affiliations; or
  - philosophical beliefs; or
  - membership of a professional or trade association; or
  - membership of a trade union; or
  - sexual orientation or practices; or
  - criminal record;
- that is also personal information; or
  - health information about an individual; or
  - genetic information about an individual that is not otherwise health information; or
  - biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
  - biometric templates.

LEX SPORTIVA

Direct marketing APP7

- General prohibition on using personal information for direct marketing, unless an exception applies
- Some common issues:
  - Databases / source of the information
  - “Opt-in” myth
  - Third-party service providers



LEX SPORTIVA

Cross–border disclosures

- Legal accountability for breaches by overseas recipients?
- A person will be an overseas recipient where they are:
- not in Australia; and
- not the entity or the individual
- Is personal information disclosed or transferred?

LEX SPORTIVA

Commissioner's expanded powers

- Power to
  - investigate and monitor compliance with APP obligations
  - conduct privacy performance assessments
  - penalties & enforceable undertakings
    - $340,000 individuals
    - $1.7million corporates

  for serious or repeated interferences with privacy

LEX SPORTIVA

Case study

- Sony PlayStation Network is an online gaming system
- Individuals' personal data provided to Sony is stored in California
- In 2011, data was accessed without authorisation. 77 million people affected worldwide, including Australians:
  - Name, address (city, state, post code)
  - Email
  - Date of birth
  - Online ID (password & login) and
  - 12,000 credit card details stolen

LEX SPORTIVA

Case study

- Sony able to demonstrate the following "reasonable steps":
  - Physical security measures (authorised users only in premises, secure storage & destruction facilities)
  - Communication security measures (encrypted email systems)
  - Network security measures (documented protocols & procedures re staff access & use of customer PI)
  - encryption of credit card information
  - internal information technology st
    based on international security st

LEX SPORTIVA

Case study

- Furthermore, as a result of attack, Sony also implemented:
  - additional data monitoring software and configuration management systems
  - increased levels of data protection and encryption
  - enhanced system monitoring, particular in terms of intrusions
  - additional firewalls
  - newly created position of Chief Information Security Officer

LEX SPORTIVA

PlayStation™

PLAYSTATION® Network

Case study

- Privacy Commissioner held:
  - Sony was subject to a targeted attack
  - Sony had, and was continuing to take, reasonable steps to protect the information
  - No penalty imposed in Australia
- However…

LEX SPORTIVA

Sony estimated $170 million loss

Sony has been fined £250,000 by the Information Commissioner's Office (ICO) following the hacking of its PlayStation Network in April 2011.

The breach compromised the personal information of millions of customers, including their names, addresses, email addresses, dates of birth, account passwords and credit card details, violating the Data Protection Act.

THE TIMES

Technology

Sony agrees to pay £250,000 fine for PlayStation Network breach

Some 70 million gaming fanatics worldwide who used the service to play online were locked out for six days

Murad Ahmed, Technology Reporter
Last updated at 3.24PM, July 15 2013

Sony has accepted a fine from UK regulators following months of fighting its penalty for allowing the personal details of millions of customers to be exposed by hackers.

LEX SPORTIVA

Notifiable data breaches

- A notifiable data breaches scheme commenced in Australia on 22 February 2018
- Applies to ‘eligible data breaches’—where the breach is likely to result in serious harm to any of the individuals to whom the information relates
- APP entities must provide a statement to the Commissioner notifying of an eligible data breach as soon as practicable after the entity becomes aware of the breach. It also requires entities to notify affected individuals as soon as practicable after preparing the statement for the Commissioner

LEX SPORTIVA

Other issues

- GDPR (EU)
- APP entities), may need to comply with the GDPR if they:
  - have an establishment in the EU (regardless of whether they process personal data in the EU), or
  - do not have an establishment in the EU, but offer goods and services or monitor the behaviour of individuals in the EU
- Access to Information
  - *Government Information (Public Access) Act 2009 (NSW)*

LEX SPORTIVA

Take home messages

- How to ensure compliance
  - Are you an APP entity? Relationship with NSO?
  - review and update standard privacy documentation (policies, collection notices and consents)
  - identify “lifecycle” of personal information
  - review business processes e.g. security measures and retention policies
  - update internal documents
  - undertake staff training
  - contracts with service providers, including in relation to OS disclosure

LEX SPORTIVA

Discussion and questions

LEX SPORTIVA

Ian Fullagar
Lex Sportiva

M: 0428 082 087
lexsportiva@icloud.com