Office of the Information Commissioner
Queensland

Over-Collection, Over-Retention, Breach – the Triple Threat of Information Privacy Protection

National Association of Field Educators

Cairns

20 October 2023

The OIC acknowledges the Traditional Owners of country throughout Australia, and their connection to land and community. We pay our respects to all Traditional Owners, and Elders past, present and emerging.

Queensland Government

Privacy Protection in Australia

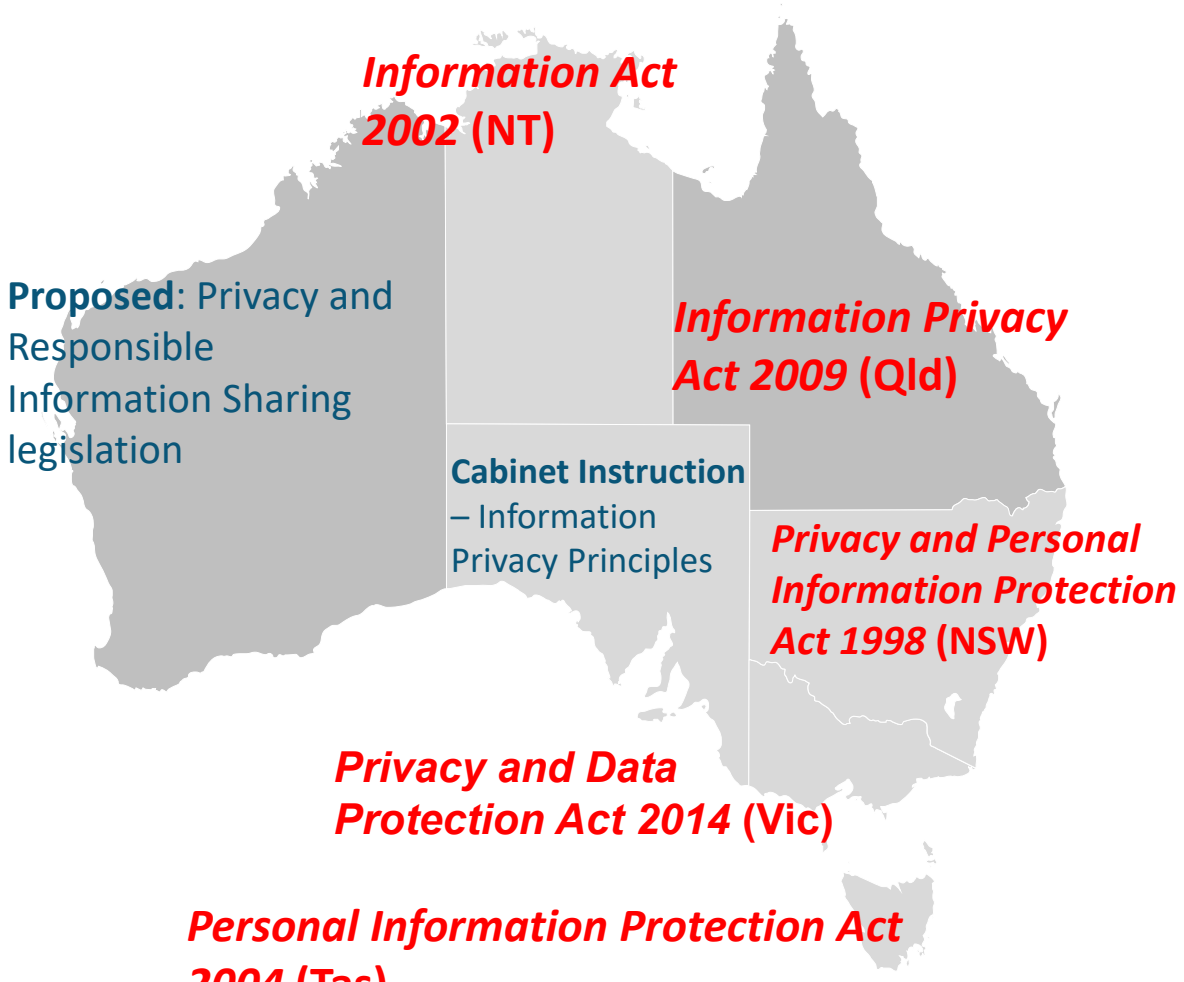
Commonwealth & Private Sector:

Privacy Act 1988

ACT

Information Act 2014

Privacy



Office of the Information Commissioner
Queensland

Office of the Information Commissioner
Queensland

Role and functions of OIC

- Independent statutory body
- OIC's statutory functions include:
  - Mediating privacy complaints against *Queensland* government agencies
  - Issuing guidelines on privacy best practice
  - Initiating privacy education and training
  - Conducting audits and reviews to monitor agency performance and compliance with the RTI Act and IP Act.
  - Review decisions of agencies and Ministers about access to, and amendment of, information under the RTI and IP Act.

Office of the Information Commissioner
Queensland

Information Privacy Act 2009 (Qld)

3 Object of Act

(1) The primary object of this Act is to provide for—

(a) the fair collection and handling in the public sector environment of personal information…

Office of the Information Commissioner
Queensland

WHAT IS PERSONAL INFORMATION?

information about a person that identifies them or allows them to be identified

not limited to name and contact information

could be information that, when combined with other information allows a person to be identified

Let's get personal …

Office of the Information Commissioner
Queensland

The privacy principles

IPPs 1 – 3 : deal with collection of personal information

IPP 4 : Storage and security

IPPs 5 – 7 : access to and amendment of documents containing personal information

IPP 8 - 9 : accuracy and relevance

IPP 10 – 11 : use and disclosure

The Triple Threats…

- Over-collection
- Over-retention
- Breaches

Office of the Information Commissioner
Queensland

Over-collection

- You should only collect personal information that is reasonably necessary to carry out your functions or activities.

- Once you hold personal information, you are responsible for safeguarding through the holding lifecycle.

- Collecting more than you need expands the ‘honeypot’, increases security requirements and inflates the risk of harm to the individual

https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/guide-to-securing-personal-information#the-information-lifecycle

Collection and ID

*The **minimum amount** of personal information needed to establish an individual's identity **should be sought**. Where possible, the personal information **should be sighted rather than copied** or collected for inclusion in a record.*

https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-12-app-12-access-to-personal-information

Collection and ID

- If you don't hold it, you can't mishandle it!

- ***Consider carefully***:
  - what personal information you require to carry out your responsibilities

  - Are there alternatives to collection?

https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/guide-to-securing-personal-information#what-is-personal-information-security

Office of the Information Commissioner
Queensland

By way of example…

OIC – Guidelines – Identity and authority for making RTI access applications

- *"If the agency has public facing offices, the original identification documents could be shown to an agency officer, who could make a file note confirming the original documents have been sighted."*

- *"Video tools - Agencies can also sight an applicant's or agent's identity using video conferencing, after which decision makers can file note that they have seen the applicant's or agent's ID."*

https://www.oic.qld.gov.au/guidelines/for-government/access-and-amendment/receiving-and-assessing-applications/evidence-of-authority-and-identity

Office of the Information Commissioner
Queensland

Over-retention

"Personal information is at risk when agencies do not have an effective disposal program in place and continue to hold public records for longer than the required minimum legal retention period."

https://prov.vic.gov.au/recordkeeping-government/a-z-topics/privacy-and-recordkeeping-obligations

Office of the Information Commissioner
Queensland

Breaches

"A data breach happens when personal information is accessed, disclosed without authorisation or is lost"

Office of the Australian Information Commissioner

Service NSW

Date: April 2020

Impact: 104,000 people

47 Service NSW staff email accounts were hacked through a series of phishing attacks. This led to 5 million documents being accessed, 10 percent of which contains sensitive data impacting 104,000 people.

A major contributing factor to the seamless breach was the l
authentication

Office of the Information Commissioner

AMBULANCE TASMANIA

Date: January 2021

Impact: Every resident that requested an ambulance between Nov 2020 and Jan 2021.

At the time of the breach, the Tasmanian ambulance was using outdated radio technology to run its communications network. Cyberattackers intercepted the radio data, converted the conversation to text, and posted the stolen data online.

Office of the Information Commissioner
Queensland

QUT

- Experienced ‘major cyber incident’ late December 2022
- Orchestrated criminal cyber attack – not human error
- Over 150 QUT systems taken off-line or unavailable
- 10 crisis management meetings between 22 December 2022 and 17 January 2023

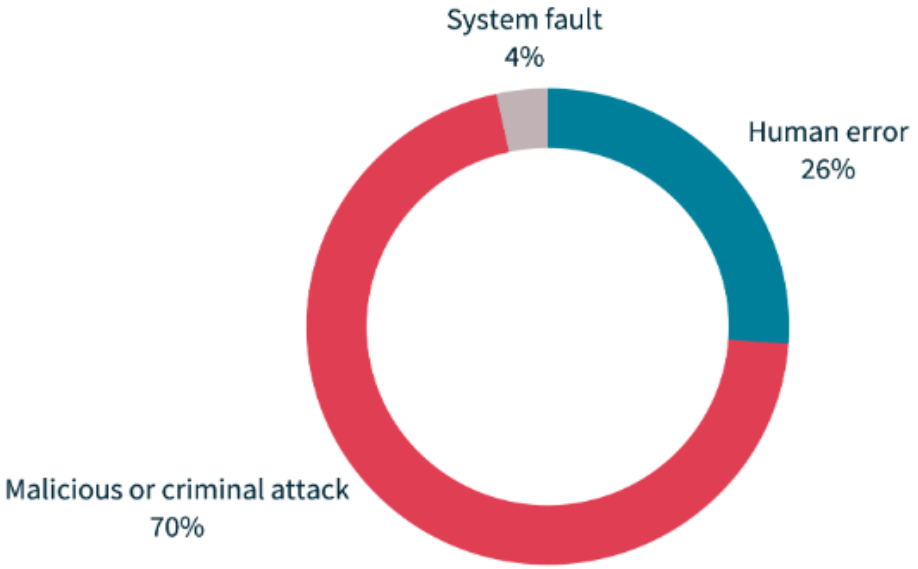
Office of the Information Commissioner
Queensland

Ones that didn't make the headlines…

- Camera containing footage of customers and staff went missing
- Outlook **auto-populating email** addresses
- Sharing the 'wrong' document containing personal information **during a Teams call**
- Patient 'hand-over' notes being dropped outside the hospital

Office of the Information Commissioner
Queensland

Sources of data breaches



Top causes of human error breaches

PI sent to wrong recipient (email) 46%

Unauthorised disclosure (unintended release or publication) 18%

Loss of paperwork / data storage device 9%

Source: OAIC Notifiable Data Breaches Report: January to June 2023: https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2023

Office of the Information Commissioner
Queensland

Consequences

Privacy breaches can have substantial impacts on *individuals* :

- Unwanted marketing and spam email
- Reputational damage
- Embarrassment or humiliation
- Identity theft or fraud
- Financial loss
- Physical harm

…and *organisations:*

- Responding to the initial breach and subsequent complaints may have financial, legal and resource implications -
- Shut downs, systems offline, logistical complications
- Financial impact - average cost of breach in Australia is $**3.35M**
- Reputational cost, including loss of public trust

What can I do?

Office of the Information Commissioner
Queensland

- **Consider collection carefully**: only collect that which you need – think ‘lightweight’

- **Keep info organised, keep info secure** - hold in as few places as possible, know your organisation’s security protocols/practices/requirements

- **Limit use and disclosure**

- **Practice information hygiene**: clean things up, don't hold on because it might be useful.

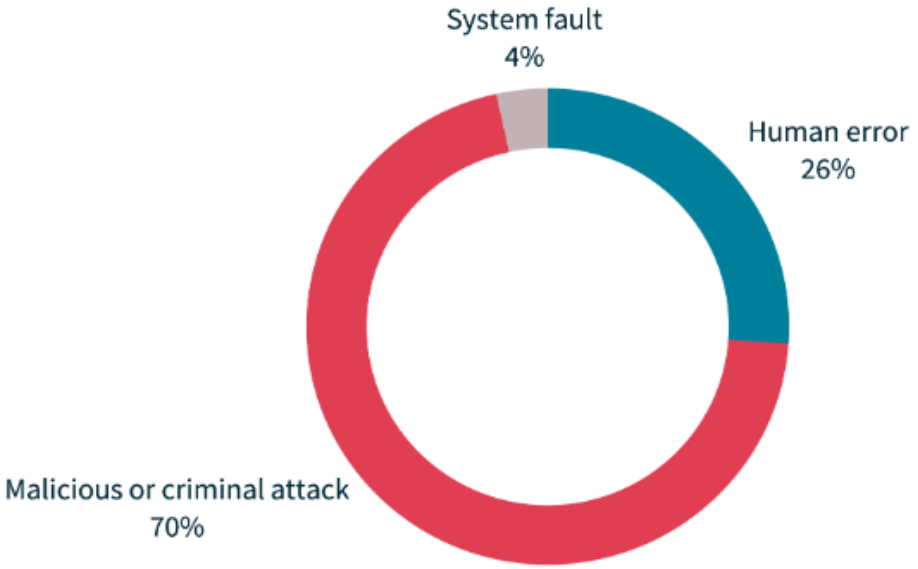
- **Stay up to date**: fluid landscape – what’s happening in your jurisdiction?

And…

Turn off auto-complete!

Office of the Information Commissioner
Queensland

Sources of data breaches



Top causes of human error breaches

PI sent to wrong recipient (email) 46%

Unauthorised disclosure (unintended release or publication) 18%

Loss of paperwork / data storage device 9%

Source: OAIC Notifiable Data Breaches Report: January to June 2023: https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2023

Office of the Information Commissioner
Queensland

OIC

- Enquiry service Tel: 3234 7373
  Email: enquiries@oic.qld.gov.au

- Subscribe to OIC News or follow OIC on 

- Guidelines and Information Sheets available at www.oic.qld.gov.au