Information Security - Data Science

MACQUARIE University

MACQUARIE University

Information Security vs Privacy

Principles Security

Principles for Data Protection

Data Protection Trade-Offs

Optus Data Breach

MACQUARIE University

Make a payment | Login to ACMA Assist

Australian Government | acma Australian Communications and Media Authority

Search the site

BetStop – The National Self Exclusion Register is now live, sign up or find out more at BetStop.gov.au

Home >

Optus data breach

If you think you may be affected by the recent Optus data breach contact Optus customer service on 133 937.

You should also:

- secure and monitor your devices and accounts for unusual activity, and ensure they have the latest security updates
- enable multi-factor authentication for all accounts
- if you need assistance with taking these steps, please visit cyber.gov.au.

Be alert for scams referencing the Optus data breach. Learn how to protect yourself from scams by visiting www.scamwatch.gov.au.

If you are concerned that your identity has been compromised or you have been a victim of a scam, contact your bank immediately and call IDCARE on 1800 595 160.

If your identity has been stolen, you can apply for a Commonwealth Victims' Certificate.

If you believe you are victim of a cybercrime, go to ReportCyber at cyber.gov.au.

The following websites can help you protect yourself and stay informed:

Why was this a privacy breach and not a security breach?

https://www.acma.gov.au/optus-data-breach

Medibank Data Breach

MACQUARIE University

Medibank hack: Russian sanctioned over Australia's worst data breach

23 January 2024

Share

By Tiffanie Turnbull, BBC News, Sydney

A Russian man has been named and sanctioned for his role in Australia's worst data breach.

The personal information of 9.7m Australians was stolen from the country's largest health insurer, Medibank, in late 2022.

Sensitive documents, including abortion records, were then posted online.

The cyber sanctions - the first of their kind in Australia - include financial penalties and a travel ban for Aleksandr Ermakov.

Little has been made public about Mr Ermakov, but Australian intelligence authorities say he is part of the infamous Russian cyber-crime gang REvil - which has been linked to attacks across Europe, the US and UK.

Announcing the measures on Tuesday, Home Affairs Minister Clare O'Neil described the Medibank hack as "the single most devastating cyber-attack we have experienced as a nation".

https://www.bbc.com/news/world-australia-68064850

How would you prevent such a breach?

Data Privacy

MACQUARIE University

How should personal data which cannot be de-identified be protected?

Australian Government
Office of the Australian Information Commissioner

Search...

Home | Privacy | Freedom of information | Consumer Data Right | Engage with us | Newsroom | About the OAIC | Contact us

Privacy > Privacy guidance for organisations and government agencies > Handling personal information > De-identification and the Privacy Act

De-identification and the Privacy Act

Key points

- De-identification is a privacy-enhancing tool. When done well, it can help your entity meet its obligations under the Privacy Act and build trust in your data governance practices.
- Information that has undergone an appropriate and robust de-identification process is not personal information, and is therefore not subject to the *Privacy Act 1988* (Cth). Whether information is personal or de-identified will depend on the context. Information will be de-identified where the risk of an individual being re-identified in the data is very low in the relevant release context (or data access environment).[1] Put another way, information will be de-identified where there is no reasonable likelihood of re-identification occurring.
- De-identification involves two steps. The first is the removal of direct identifiers. The second is taking one or both of the following additional steps:
  - the removal or alteration of other information that could potentially be used to re-identify an individual, and/or
  - the use of controls and safeguards in the data access environment to prevent re-identification.
- This guide provides high-level guidance only. The OAIC recommends that entities also refer to the De-Identification Decision-Making Framework, produced jointly by the OAIC and CSIRO-Data61, which provides a comprehensive framework for approaching de-identification in accordance with the Privacy Act.
- The OAIC recommends that entities seek specialist expertise for more complex de-identification matters - for example when de-identifying rich or detailed datasets, where data may be shared publicly or with a wide audience, or where de-identification is carried out in the context of a multi-entity data sharing arrangement.[2]

https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/de-identification-and-the-privacy-act

Information Security vs Privacy

AN EXAMPLE

Sensitive dataset

Anonymisation

De-identified (sub)-dataset

What happens to this data?

This data is safe (privacy law does not apply)

Information Security vs Privacy

MACQUARIE University

RELATION TO PRIVACY LAW

How should personal data which cannot be de-identified be protected?

Recall: Both Australian Privacy Law and GDPR are guided by the following principles

1. **Transparency** - *Includes having a clearly expressed privacy policy.*
2. **Purpose / storage limitation** - *Entities can only collect, process and store information for the stated purpose.*
3. **Integrity / accuracy** - *Data must be kept up-to-date and accurate*
4. **Confidentiality** - *Stored securely and with access controls*

Principles for Information Security and Data Protection

- based on slides by Meiko Jensen, Karlstad University, Sweden and sources from Data Privacy and Information Security Unit

Running example: customer database containing sensitive information (names, addresses, DOB, credit card details, transactions, locations).

Principles for security

CIA TRIAD

Principles for security

CONFIDENTIALITY

1. Confidentiality:

Protect private/sensitive data from unauthorised access so as to prevent accidental disclosure of sensitive information.

Also known as…

- Non-disclosure
- Secrecy
- Access restrictions
- Security clearances
- Unobservability

Principles for security

CONFIDENTIALITY

Confidentiality techniques

Think about: physical, logical, network

Encryption
- SSL/TLS
- Databases

Access control
-Physical
-Software , Access control lists

Firewalls
-Onion routing
-Passwords

```
        top secret
       /          \
classified        secret
       \          /
        public
```

Principles for security

INTEGRITY

2. Integrity:

Protect private/sensitive data from unauthorised modification or undetected modification.

Also known as...

- Authenticity
- Non-repudiation
- Detection of data changes
- Reliability
- Resilience

Principles for security

INTEGRITY

Integrity techniques

Think about: physical, logical, network

Hashes / checksums
- Md5

Access controls

Secure backups

Account logging and monitoring

Blockchain

Principles for security

AVAILABILITY

3. Availability:

Ensure that access to private/sensitive data is granted in a timely, comprehensible and processable manner.

Also known as…

- Redundancy
- Accessibility
- Responsiveness
- Uptime

Principles for security

AVAILABILITY

Availability techniques

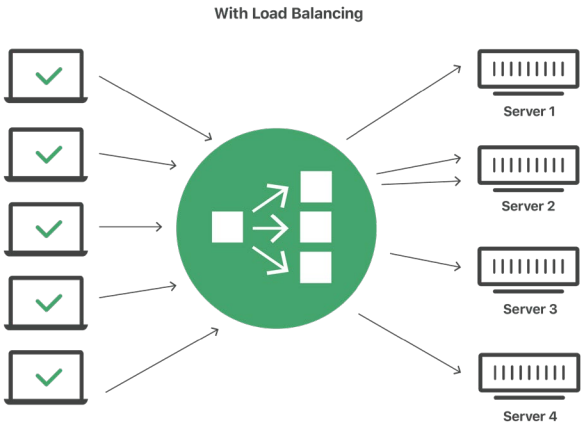
Think about: physical, logical, network

Load balancing

Backups

Failover

Redundancy



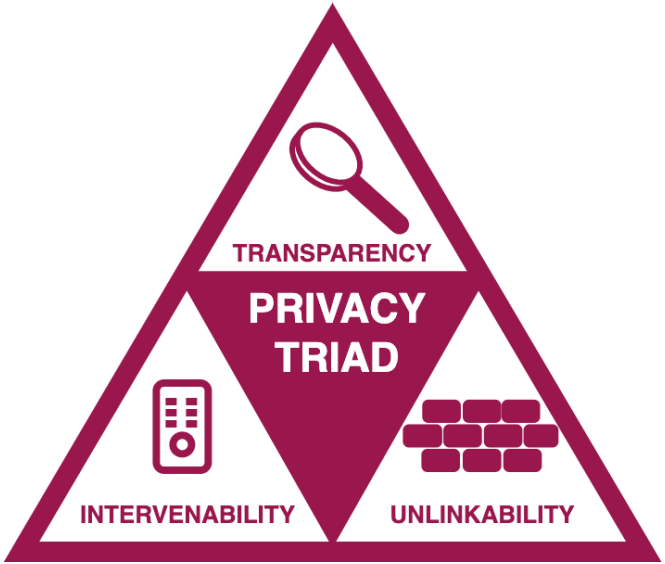
Principles for Data Protection

Principles for data protection

MACQUARIE University

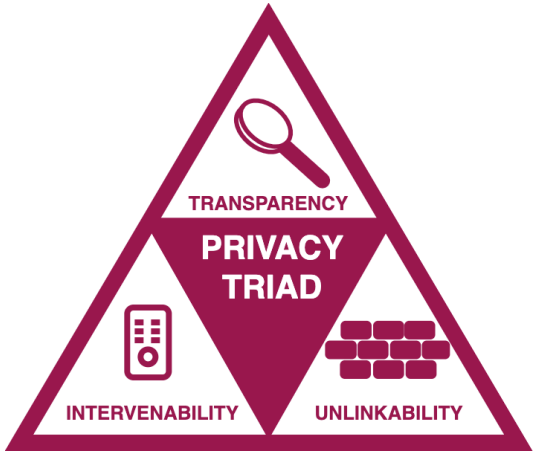
PRIVACY TRIAD?

The “privacy triad” for data protection.



Principles for data protection

TRANSPARENCY



1. Transparency:

Ensure that all privacy-relevant data processing can be understood and reconstructed at any time.

Also known as…

- Accountability
- Reproducibility
- Full-disclosure
- Auditability

Principles for data protection

MACQUARIE University

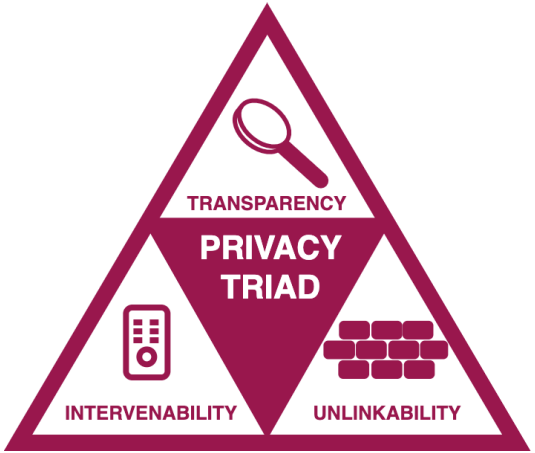
INTERVENABILITY

2. Intervenability

Grants data subjects the rights to interventions such as notification, rectification or erasure at any time.

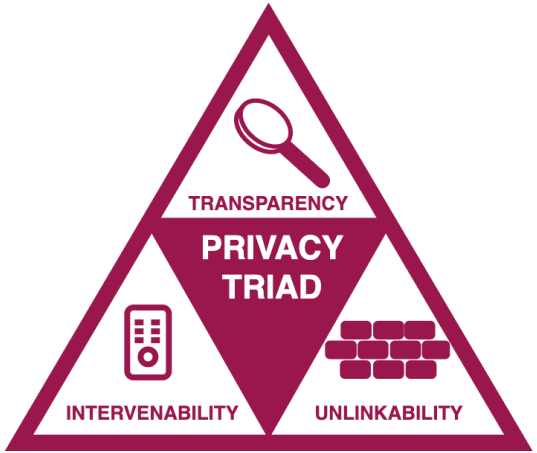
Also known as...

- Consent and consent withdrawal
- Claim lodging
- User controls
- Right to be forgotten



Principles for data protection

UNLINKABILITY



3. Unlinkability:

Ensure that all privacy-relevant data cannot be linked with other data sources to derive more detailed records.

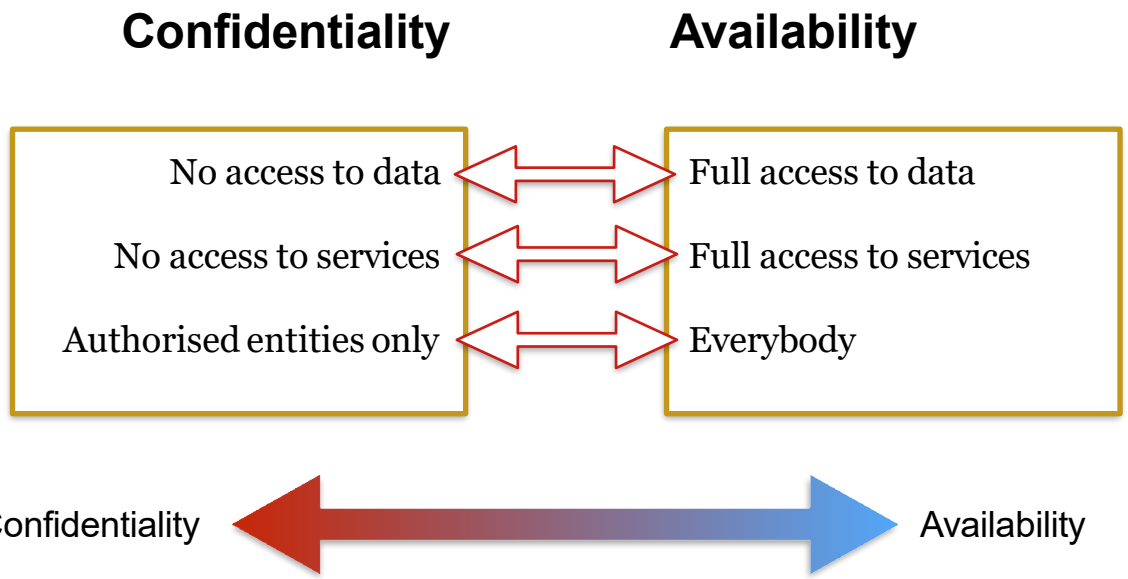
Also known as…

- Purpose limitation
- Data minimisation
- Unobservability
- Undetectability

Data Protection Trade-Offs

Data Protection Trade-Offs

CONFIDENTIALITY <-> AVAILABILITY



Data Protection Trade-Offs

MACQUARIE University

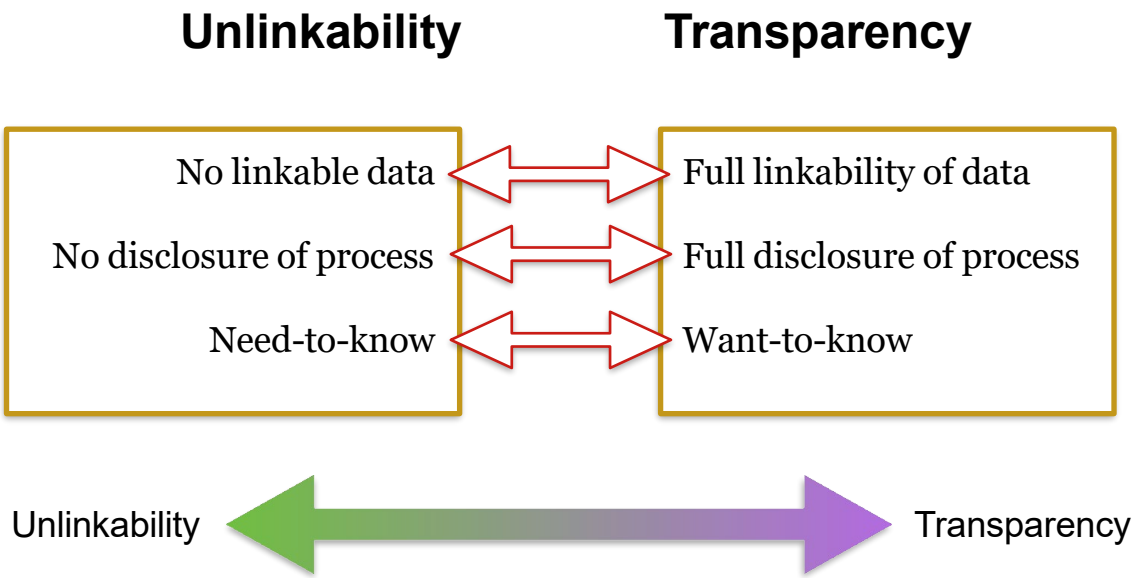
INTEGRITY <-> INTERVENABILITY

Integrity	Intervenability
No changes to data	All types of changes
No changes to process	Full process flexibility
Defined by organisation	Defined by individual

Data Protection Trade-Offs

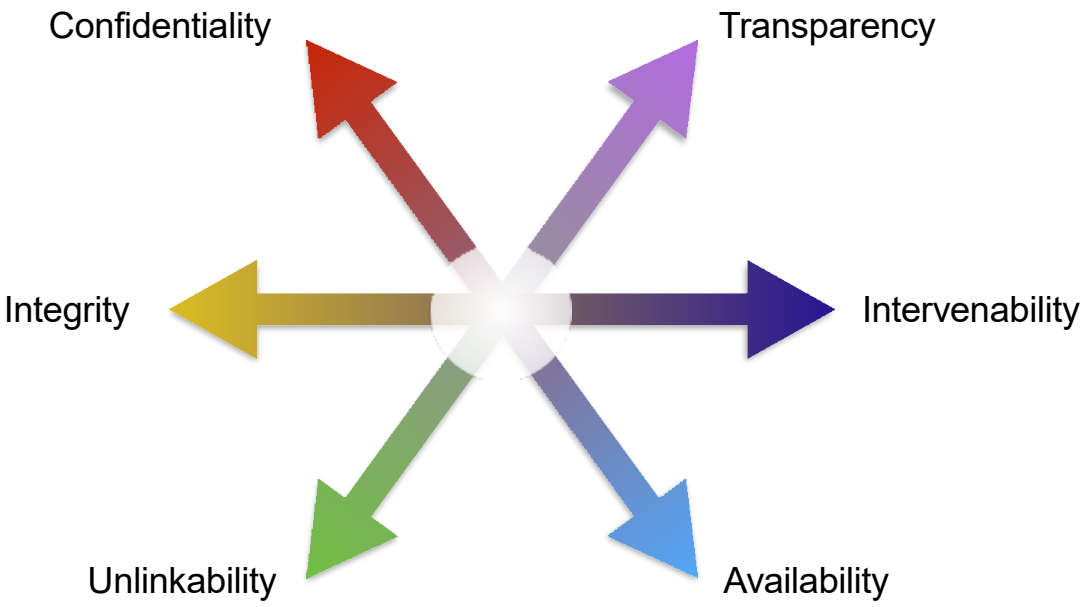
MACQUARIE University

UNLINKABILITY <-> TRANSPARENCY



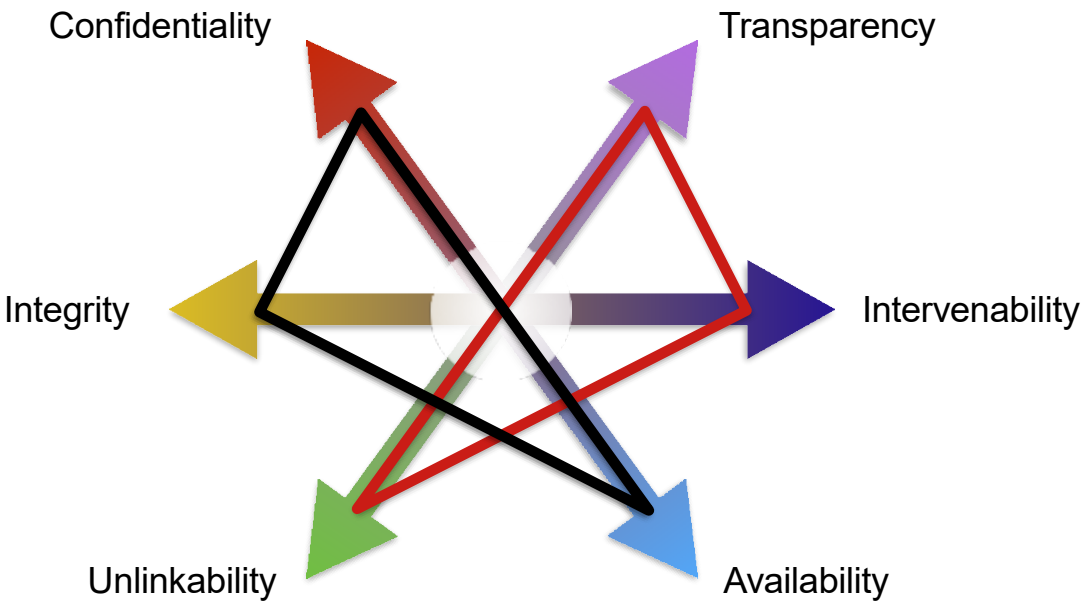
Data Protection Trade-Offs

SIX-POINTED STAR



Data Protection Trade-Offs

SIX-POINTED STAR



Modelling Data Breaches

Database containing customers' names, dates of birth, phone numbers, email addresses, medicare details, passport details and drivers licences

If you were conducting a privacy risk assessment, what questions would you ask?

Modelling Data Breaches

MACQUARIE University

If you were conducting a privacy risk assessment, what questions would you ask?

1. Create a model of the system

   - data flow diagram to model information flows and entities
   - physical model to identify security weaknesses

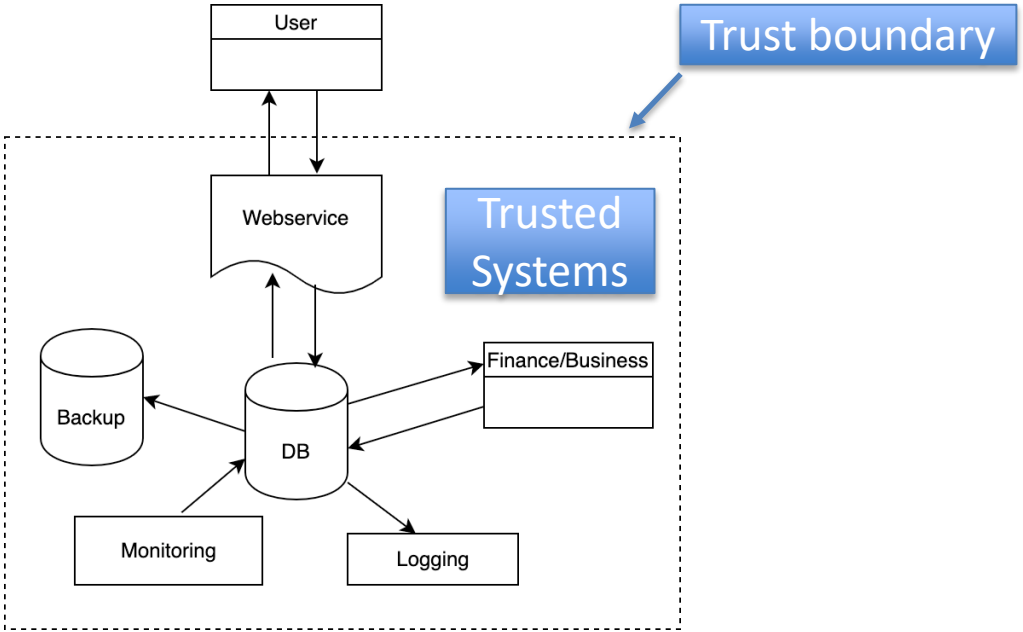
2. Use the security and privacy principles to identify potential weaknesses in the model.

3. In the case of a discovered weakness, propose solutions.

Modelling Data Breaches

MACQUARIE University

Data Flow Diagram



Modelling Data Breaches

MACQUARIE University

If you were conducting a privacy risk assessment, what questions would you ask?

Confidentiality

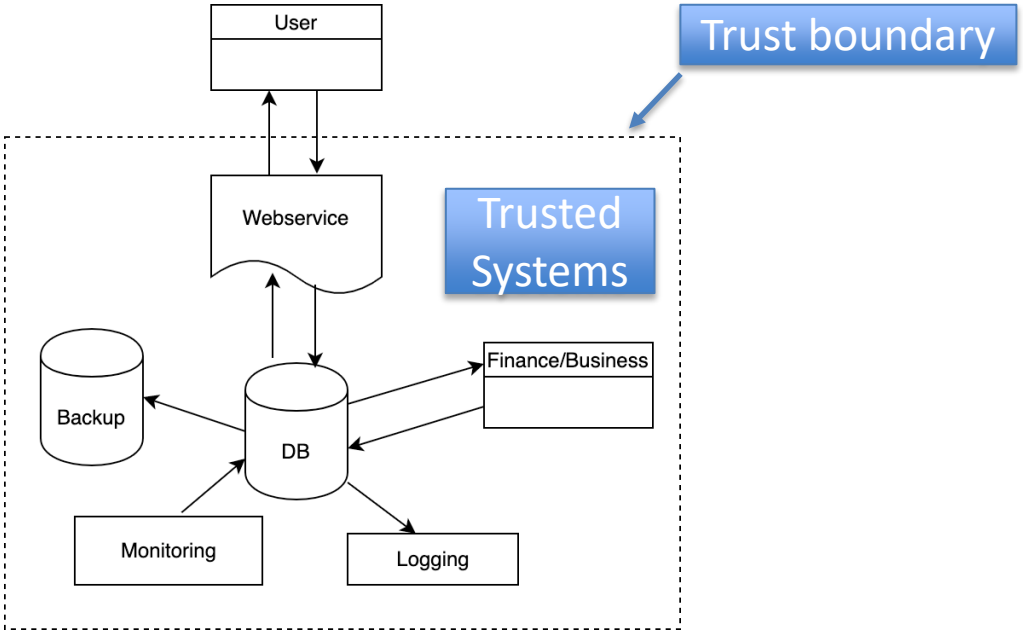
Is the connection encrypted?

Is the data encrypted?

where are the backups stored?

Who has access to the systems?

Access controls?



Modelling Data Breaches

MACQUARIE University

If you were conducting a privacy risk assessment, what questions would you ask?

Integrity

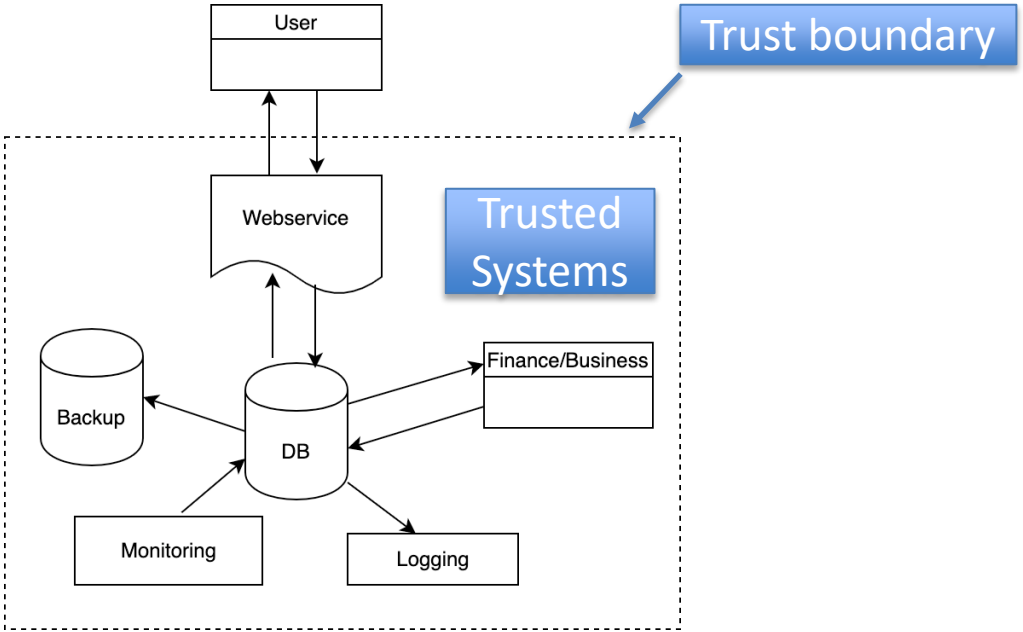
Are there identity checks?

Are there logs tracking changes?

Is there a backup policy?

Notification of transactions

MD5 hashes/ checksum on backups



Modelling Data Breaches

MACQUARIE University

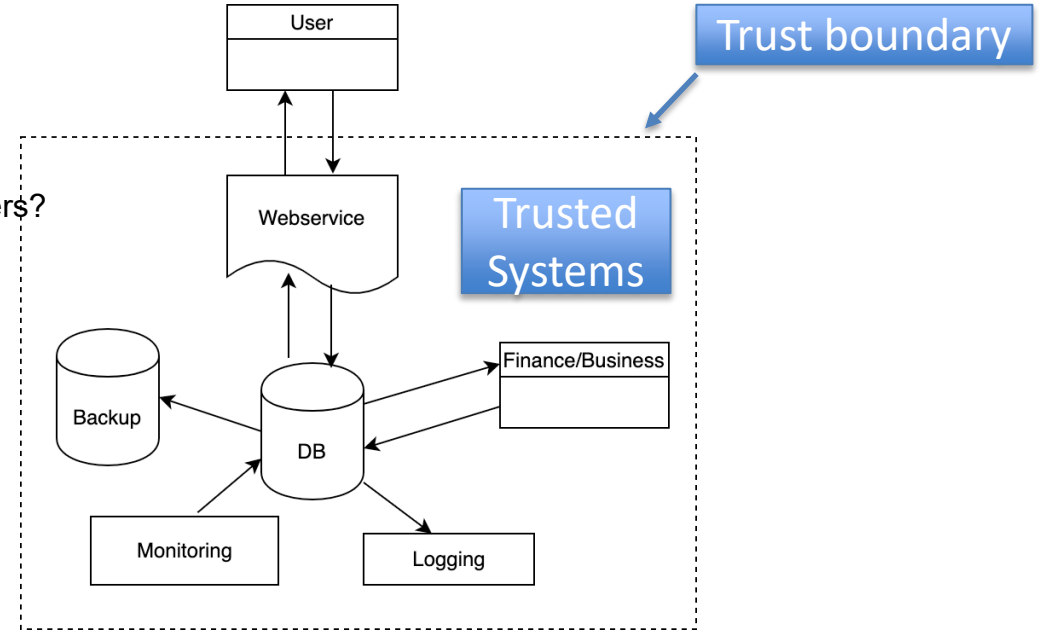
If you were conducting a privacy risk assessment, what questions would you ask?

Availability

Is there load balancing on the web servers?

What happens if the DB goes down?

What if there is a network outage?



Modelling Data Breaches

MACQUARIE University

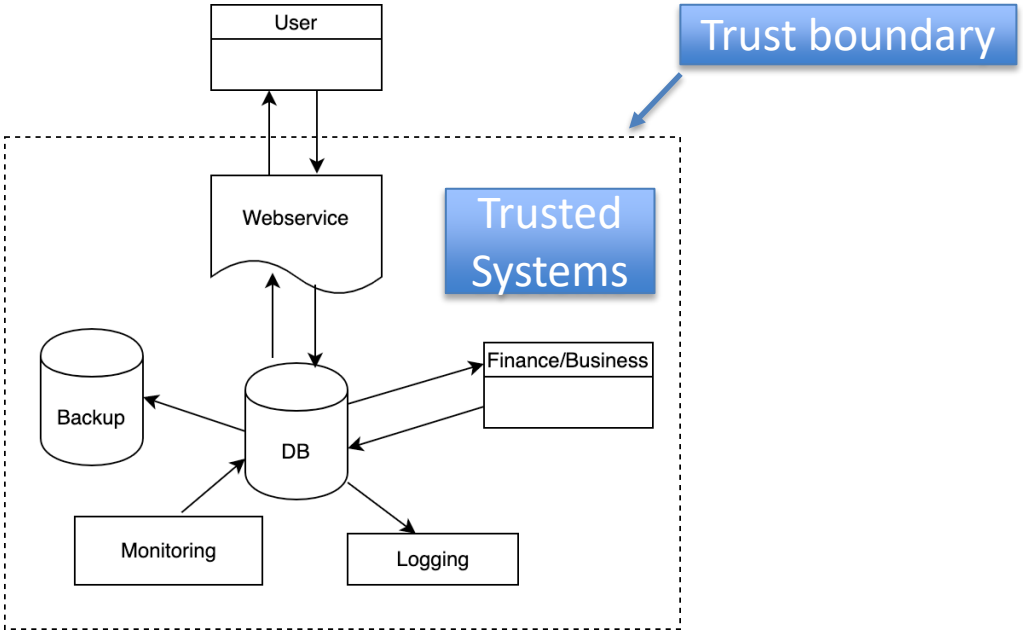
If you were conducting a privacy risk assessment, what questions would you ask?

Transparency

Do you have privacy policy?

Are you notifying uses of loggings or unusual activity?

Do you ask for cookie policy?



Modelling Data Breaches

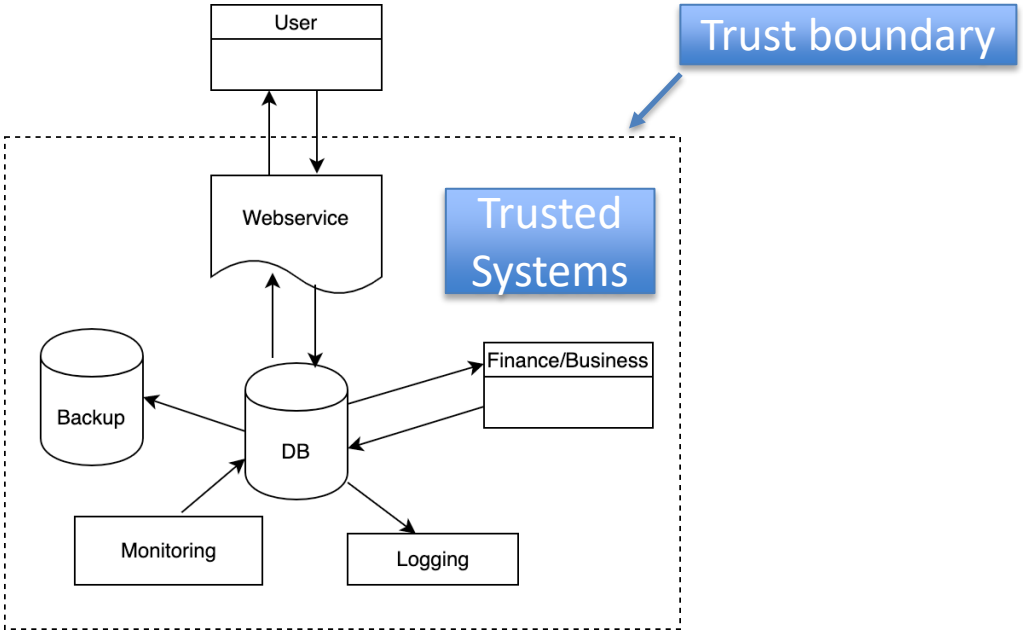
MACQUARIE University

If you were conducting a privacy risk assessment, what questions would you ask?

Intervenability

Do customers have a way to change their data?

Are changes properly synchronized?



Modelling Data Breaches

MACQUARIE University

If you were conducting a privacy risk assessment, what questions would you ask?

Unlinkability

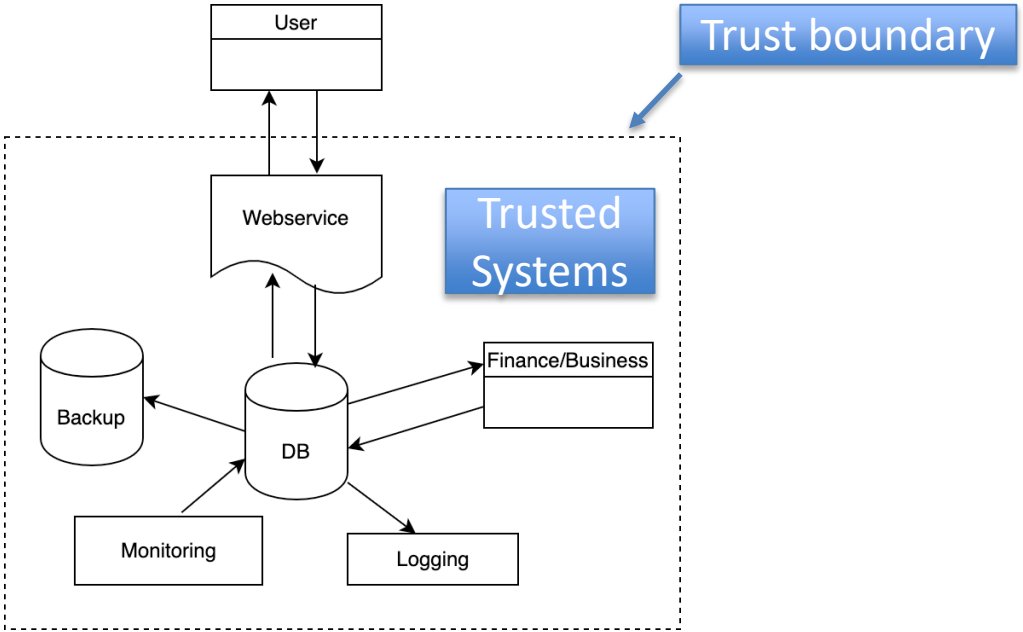
What information are you collecting?

Do you need it all?

Can some be deleted?

Are you removing common identifiers?

How is your data segregated?



Information Security vs Privacy

MACQUARIE University

SUMMARY

What we talked about today:

1. **Transparency** - *Includes having a clearly expressed privacy policy.*
2. **Purpose / storage limitation** - *Entities can only collect, process and store information for the stated purpose.*
3. **Integrity / accuracy** - *Data must be kept up-to-date and accurate*
4. **Confidentiality** - *Stored securely and with access controls*