Obfuscation-based inference controls

Obfuscation-based inference control

- **Anonymisation**
  - decoupling identification from information.
  - achieving anonymisation is extremely difficult.
  - labelling a data set as anonymised remains unclear.

- **Generalisation**
  - reducing the precision of data to reduce the likelihood of informing identity.
  - example: use of ranges.

- **Suppression**
  - suppression information, making fewer data available to attacker to reduce inferences.
  - example: suppression gender in 50% of data records.

Obfuscation-based inference control

- **Dummy addition**
  - adding *dummies* or fake data points to data sets prior to providing to other party.
  - example: artificial records.

- **Perturbation**
  - adding noise to data to reduce the ability of other party to form inferences.
  - example: differential privacy.

Obfuscation-based inference controls