Designing Privacy by Design

AusCERT 2013, Gold Coast, Queensland
23 May 2013

Stephen Wilson
Lockstep Group

Privacy ≠ Anonymity

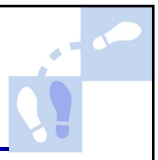
"The right to be let alone"

Warren & Brandeis (1890)

When someone knows you,
they should respect the knowledge
they have about you

Privacy is a state where a party that has Personal Information about you is constrained in how they use that information

Maybe not intuitive …



Personal Information

Information or an opinion,
whether true or not,
about an individual
whose identity is apparent,
or can reasonably be ascertained

Privacy Act 1988

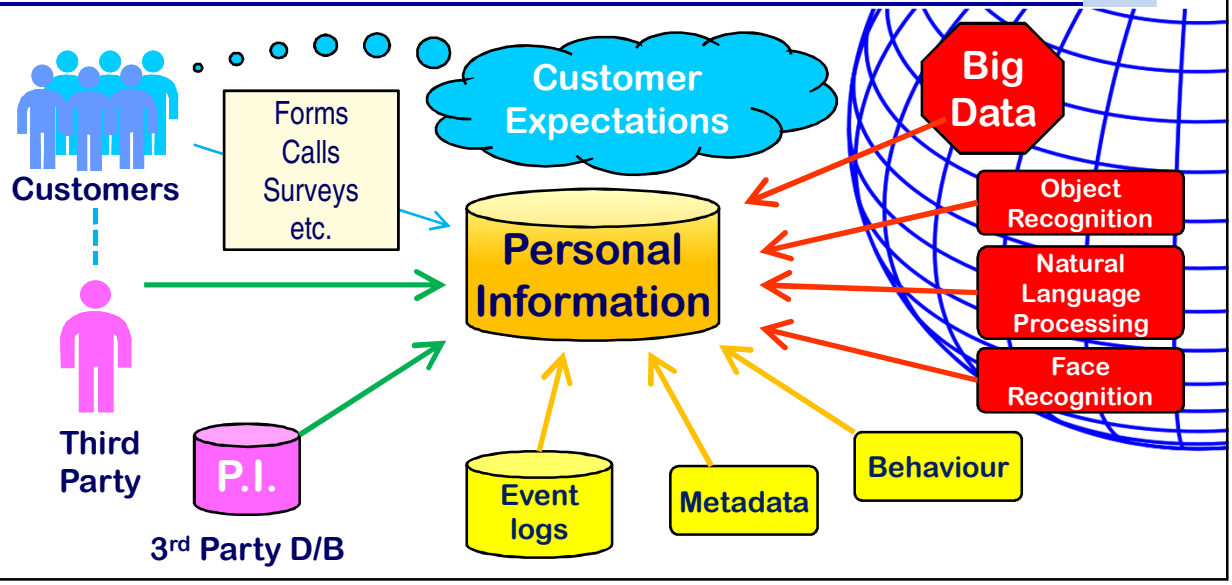
Maybe not intuitive …

Personal Information

Information or an opinion,
whether true or not,
about an individual
whose identity is apparent,
or can reasonably be ascertained

Privacy Act 1988

Collection mechanisms



Case 1: Street View Wi-Fi

- SSIDs collected to enhance geo-location
- "Accidentally" collected Wi-Fi contents
- Unencrypted data may be identifiable
- "Public domain"?
- European, Australian, US responses

Case 2: Facial recognition

- Biometric templates generated from tags
- Facial recognition creates new tag suggestions
- European regulatory decision
- In Australia, biometrics will soon be *Sensitive*

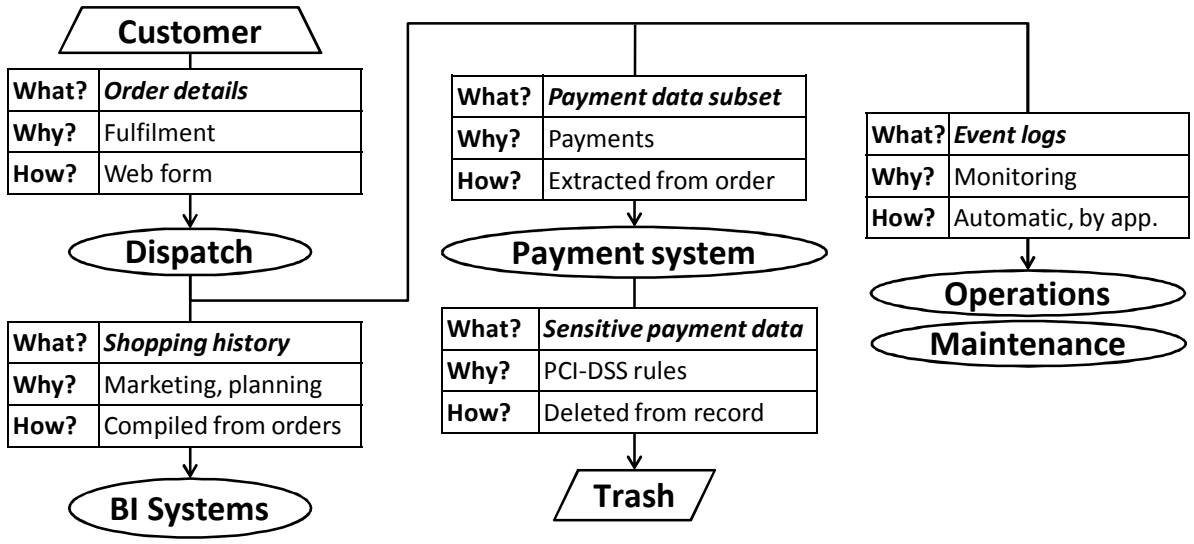
Case 3: Pregnancy predictor

- Classic Big Data
- Health Information is *Sensitive* PI
- Cannot be collected without consent
- Big Data stretches Collection Principle

Privacy Impact Assessment

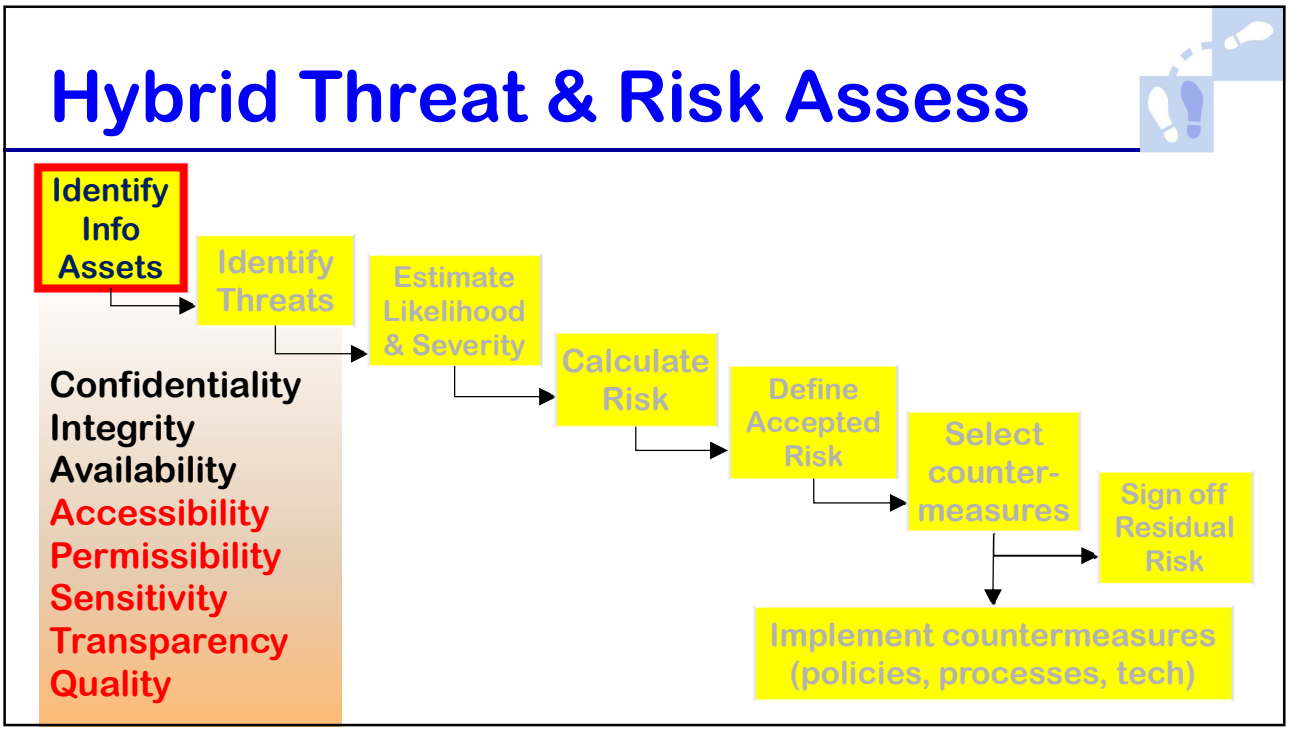
- Quasi-standardised:
  - Situation analysis
    - Information flows
      - Gap analysis against relevant Privacy Principles
        - Recommendations
- Repeat as necessary
- Classically a compliance tool
- But the sooner the better

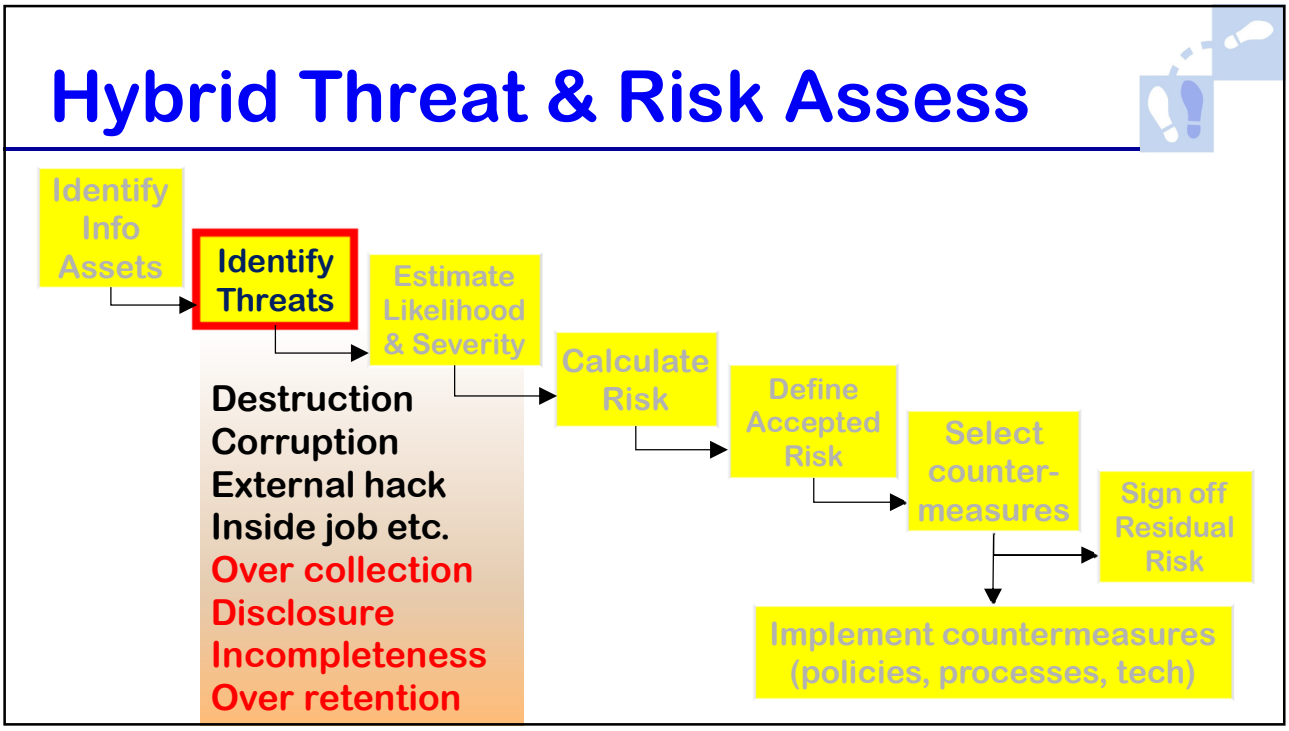
Information flow mapping



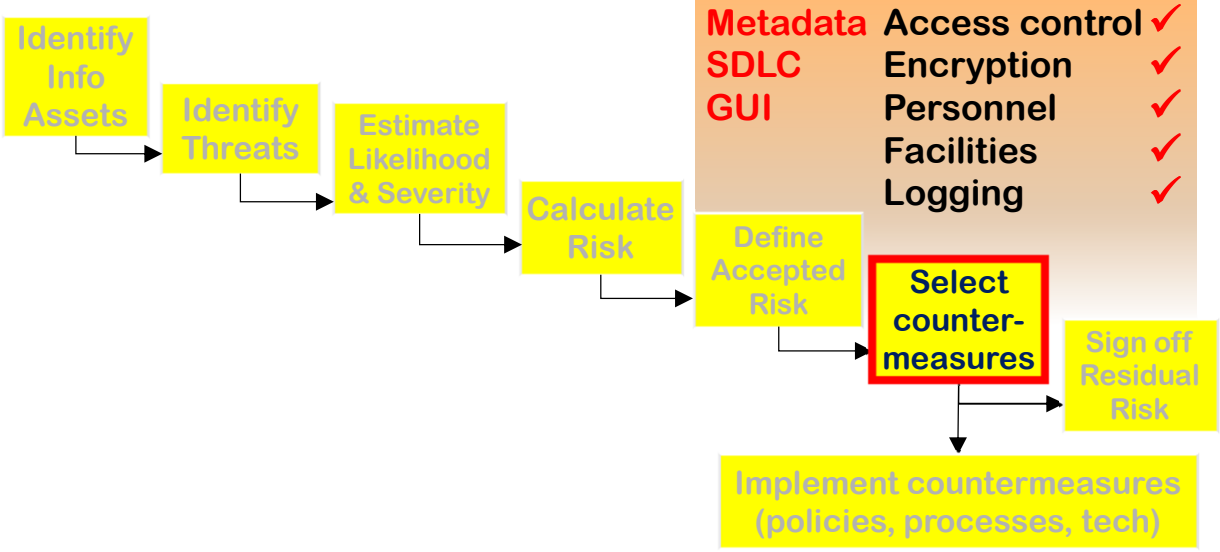
Extended Info Asset Inventory

Item	C	I	A	Personal?	Accessibility	Permissibility	Transparency	Quality	Sensitivity
Customer record									
Employee record									
Price list - products									
Price list - supplies									
Access Control List - int									
Access Control List - ext									
Commerce server event log									
Firewall rule set									
…									





Hybrid Threat & Risk Assess



Privacy is …

- Not about security
- Not about secrecy
  - Few people actually want anonymity
- All about control
- All about respect
- Reducible to engineering requirements

Further reading

- *Siri: A penny for your thoughts?* Lockstep March 2012
  http://lockstep.com.au/blog/2012/03/12/a-penny-for-your-thoughts
- *What stops Target telling you're pregnant?* Lockstep March 2012
  http://lockstep.com.au/blog/2012/03/07/target-tells-youre-pregnant
- *Not too late for privacy* Lockstep October 2012
  http://lockstep.com.au/blog/2012/10/29/not-too-late-for-privacy
- *The beginning of* privacy Lockstep February 2013
  http://lockstep.com.au/blog/2013/02/12/the-beginning-of-privacy
- *Facebook suspends photo tag tool in Europe* BBC 21 Sep 2012
  http://www.bbc.co.uk/news/technology-19675172
- DNA hacking, MIT
  http://wi.mit.edu/news/archive/2013/scientists-expose-new-vulnerabilities-security-personal-genetic-information

Discussion

swilson@lockstep.com.au
http://lockstep.com.au