Australian Government

Office of the Australian Information Commissioner

Cybersecurity Education Summit 2019

Keynote: Andrew Solomon
Assistant Commissioner, Dispute Resolution

@OAICgov

OAIC

Office of the Australian Information Commissioner

- Integrity agency, promoting transparent and accountable handling of personal information

- Human rights agency, protecting the right of individuals to personal autonomy, choice and control

- We recognise the economic value of personal information and seek outcomes in the public interest

Overview

1. What privacy means and the OAIC’s role in regulating personal privacy
2. Challenges in the current environment
3. How privacy intersects with cybersecurity

The human factor

Most data breaches reported to the OAIC involve the human factor:

- Cyber attacks
- Human error
- Some system faults

Impact of a data breach

- Time
- Money
- Emotional toll
- Potential for physical harm

@OAICgov

Impact on people

- One in four Australians have had their personal information misused
- It takes the average person more than 27 hours to keep their identity and accounts safe

Dealing with a data breach

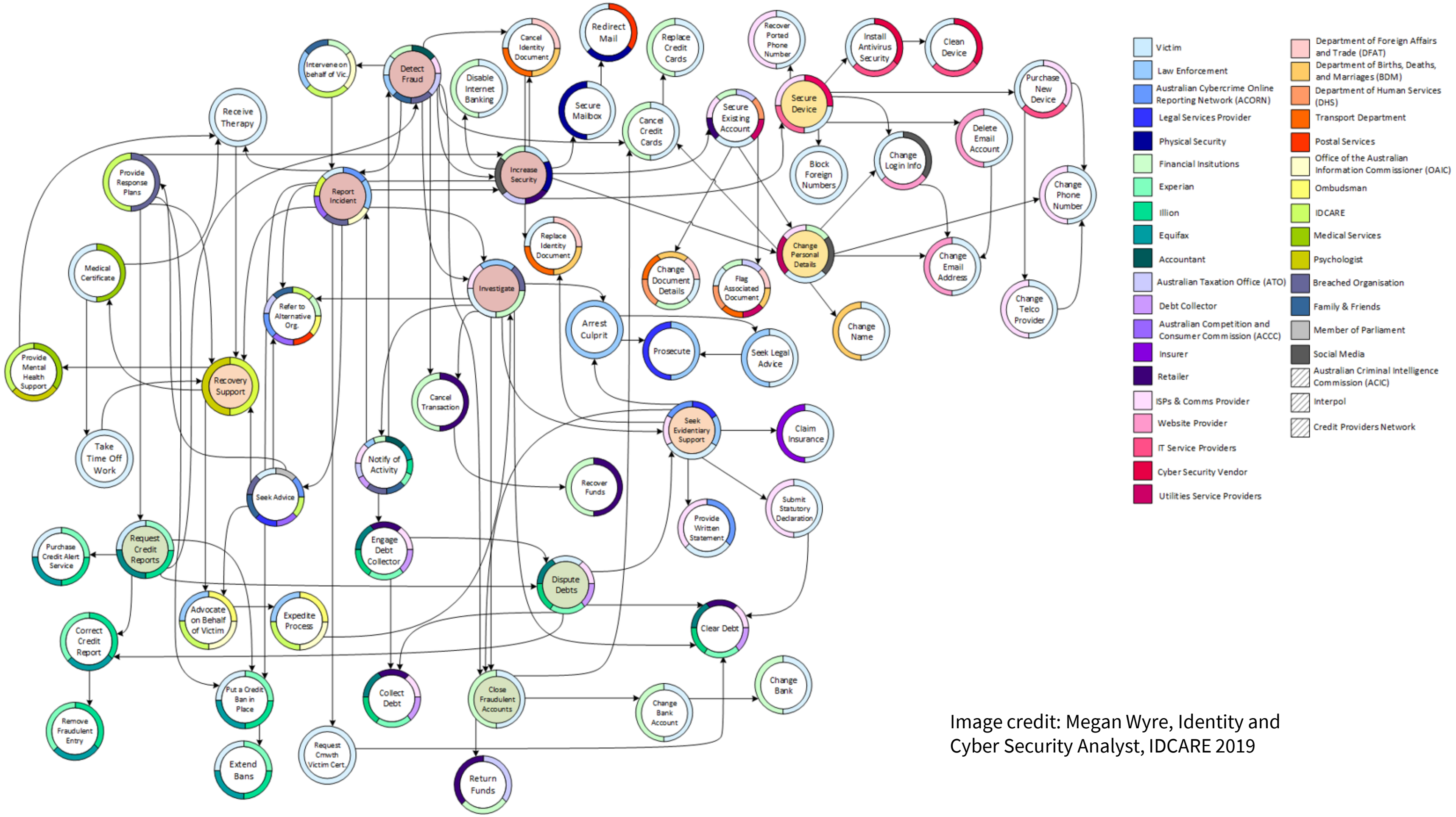


Image credit: Megan Wyre, Identity and
Cyber Security Analyst, IDCARE 2019

Cost of data breaches

Identity crime costs Australians $2.6 billion a year – *Attorney-General's Department 2016 report.*

The cost of a data breach to business is growing – an average $3 million per incident in Australia in 2019 – *IBM Security Ponemon Institute Survey.*

New system of penalties to strengthen online privacy protections

What is privacy?

A fundamental human right recognised in the UN Declaration of Human Rights.

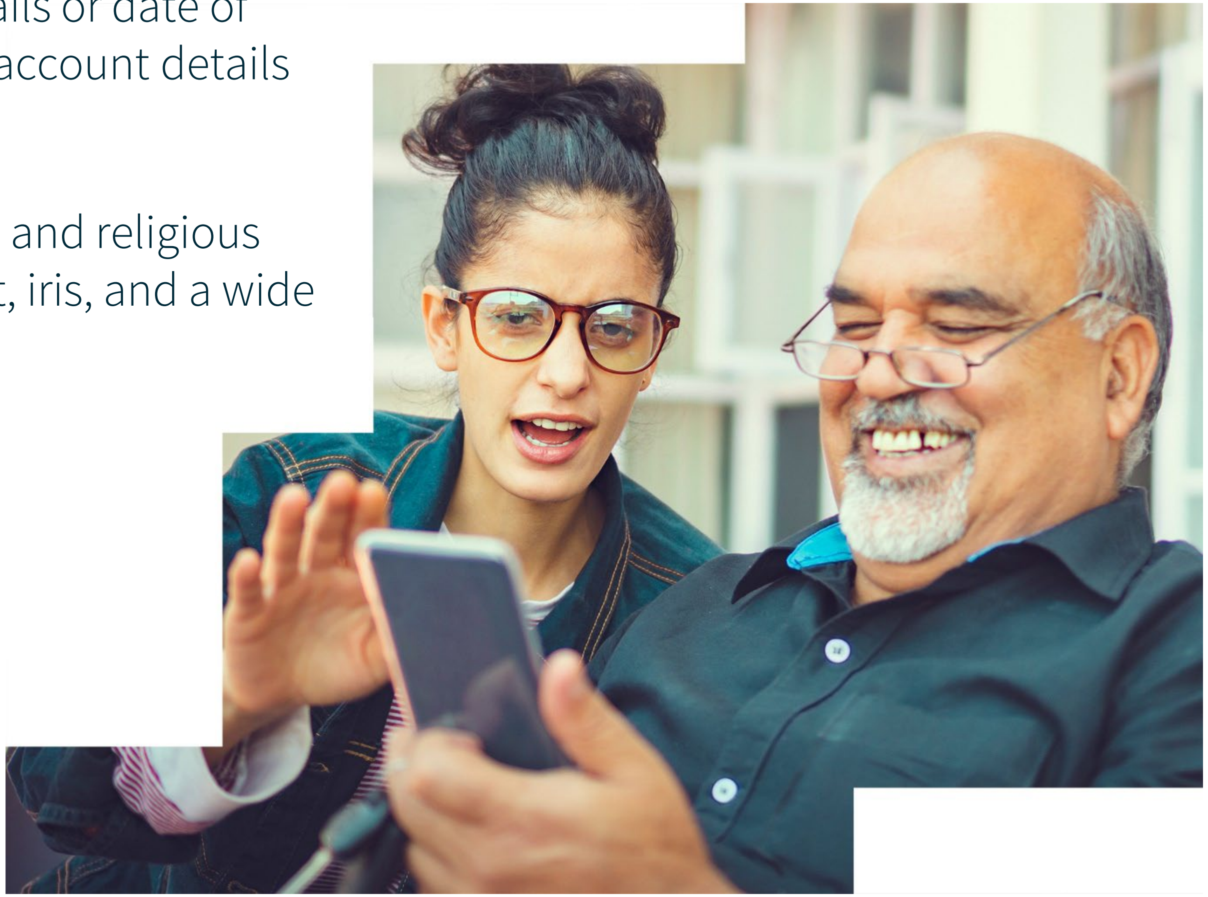
Information privacy is about protecting the collection and handling of information that says:

- who we are
- what we do
- and
- what we believe

What is personal information?

- Your name, signature, contact details or date of birth, your medical records, bank account details and credit history

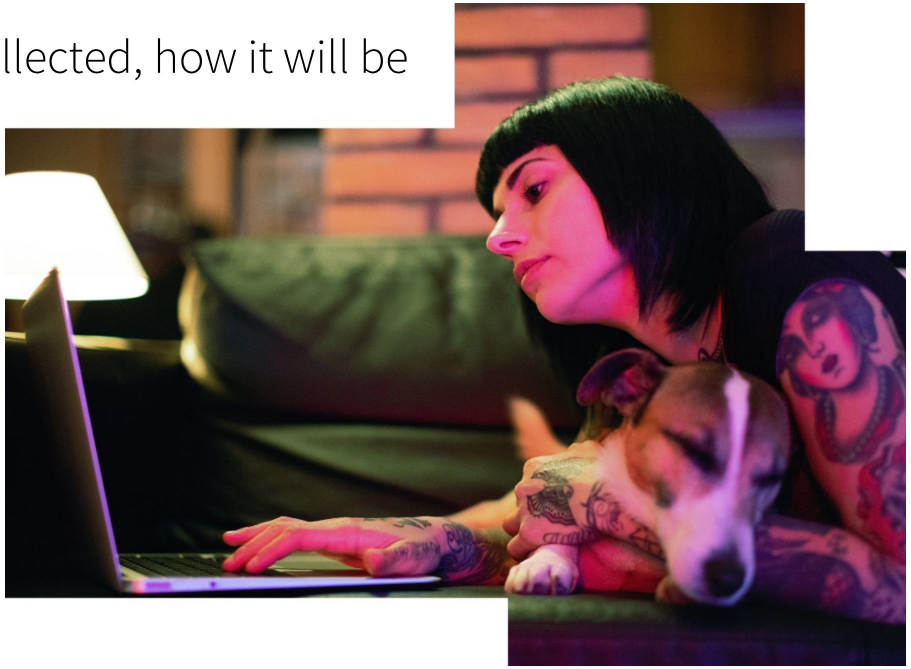
- Your photo, your political opinions and religious beliefs, your fingerprint, voice print, iris, and a wide range of other information



Privacy rights

Australia's *Privacy Act 1988* gives us the right:

- to know why our personal information is being collected, how it will be used and who it will be disclosed to
- to ask for access to our personal information, and
- for organisations to secure the information and ensure its accuracy before using or disclosing it



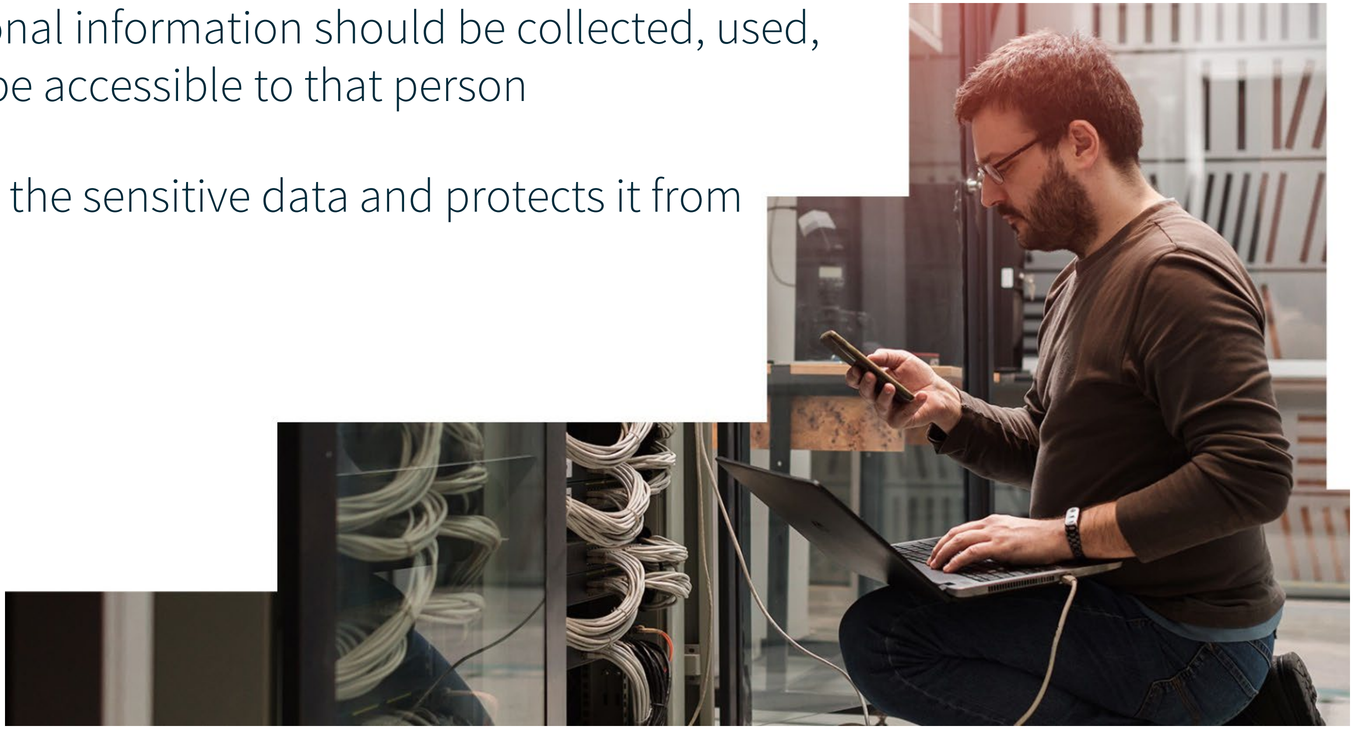
Securing personal information

- Rapid growth in value of data
- Growth in the volume of data holdings
- Rapid adoption of new technologies

@OAICgov

Interface between privacy and cybersecurity

- Cybersecurity and privacy should not be separate domains within an organisation
- Privacy governs how personal information should be collected, used, shared and retained, and be accessible to that person
- Security restricts access to the sensitive data and protects it from unauthorised access
- Each informs the other



Notifiable Data Breaches Scheme

Organisations are legally required to quickly assess actual or suspected data breaches

If serious harm is likely to result, they must notify affected individuals

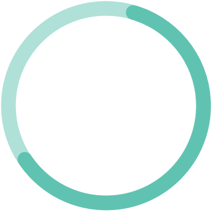
They must also notify the OAIC

Assessing harm

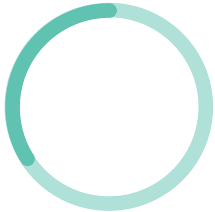
- Financial information
- Identity information
- Contact information
- Health information

NDB Statistics 2018-19

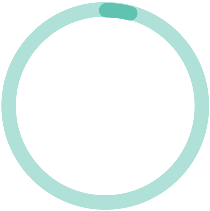
950 notifications in total



Malicious or criminal attacks are the leading cause



Human error accounts for about a third of mandatory notifications



System faults accounted for the remainder (business or technology process error)

Data breach prevention – best practice

1. Training
2. Understanding your personal information holdings
3. Preventative technologies and processes
4. Preparing and rehearsing for responding to a data breach
5. Trust and transparency – communicating clearly

Global privacy landscape

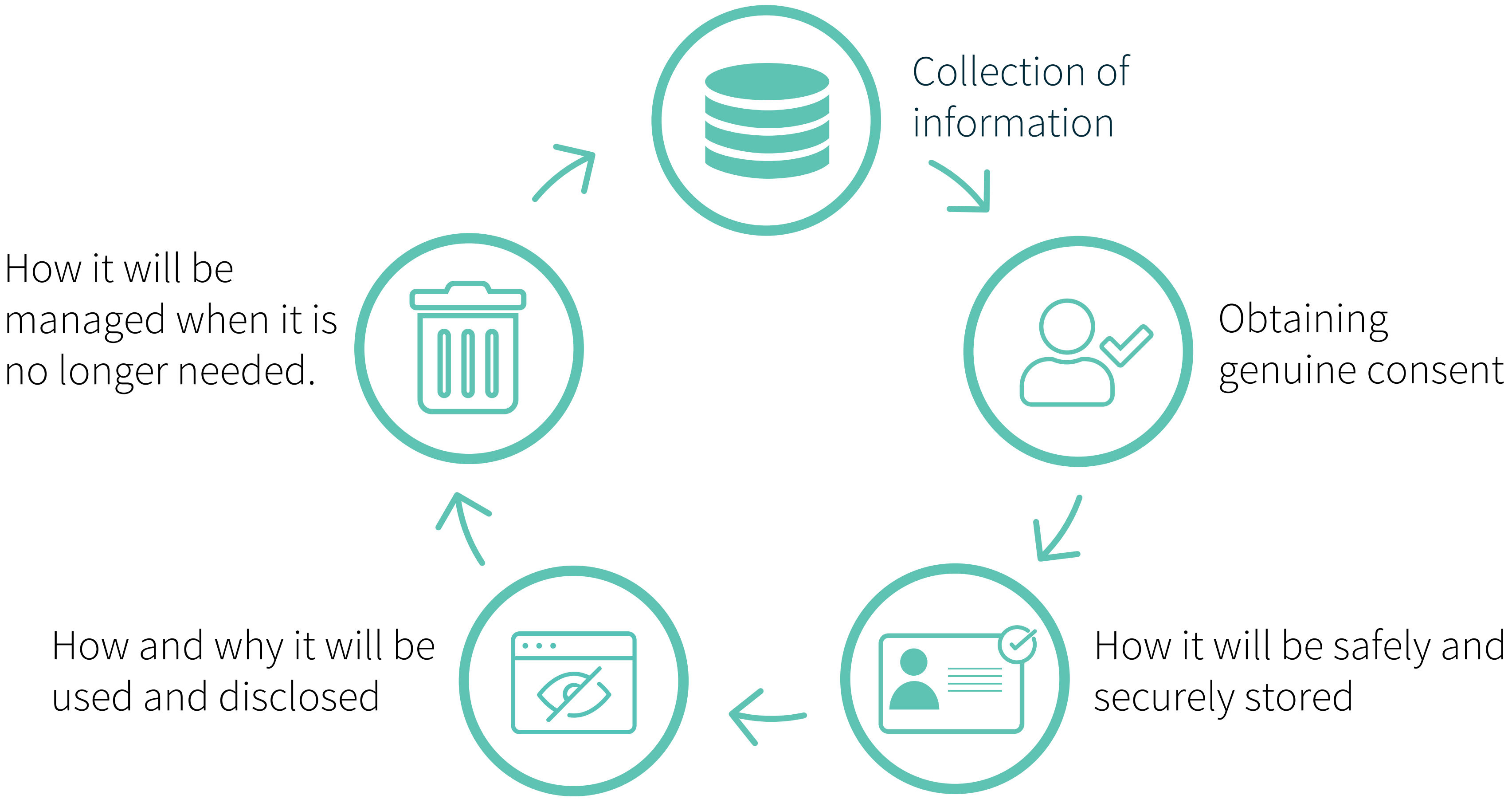
- Building privacy from the ground up
- Data knows no borders
- Working towards globally interoperable standards and enforcement
- Convergence of data and consumer protection

Looking to the future: cybersecurity education

@OAICgov

OAIC

The information life cycle



Collection of information

Obtaining genuine consent

How it will be safely and securely stored

How and why it will be used and disclosed

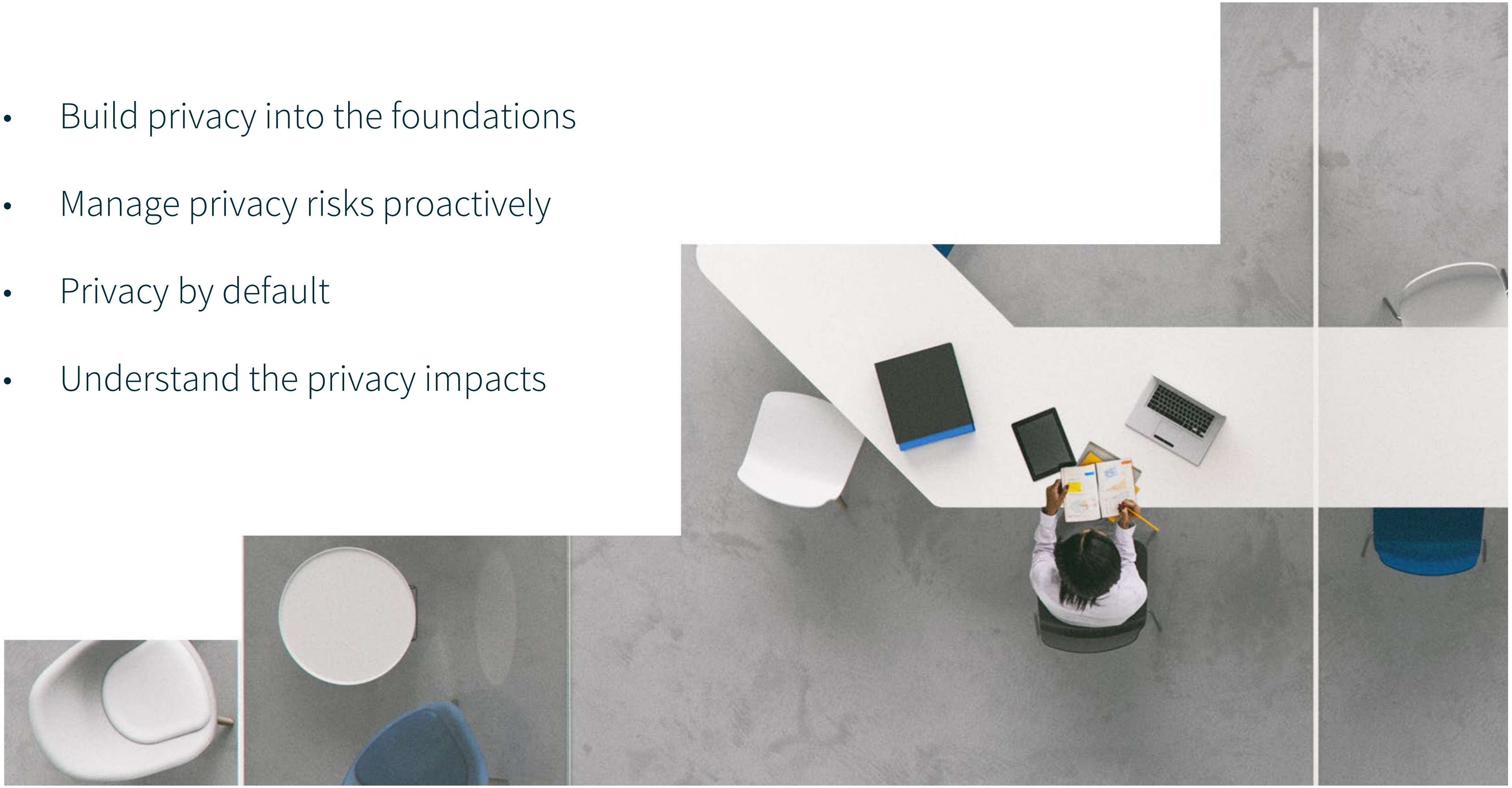
How it will be managed when it is no longer needed.

@OAICgov

OAIC

Privacy by design

- Build privacy into the foundations
- Manage privacy risks proactively
- Privacy by default
- Understand the privacy impacts



People and technology

- Understand human behaviour
- Anticipate risks
- Cybersecurity professional is also a trainer

An introduction to privacy for the cybersecurity professional

1: Privacy/cybersecurity interface

2: What is privacy

3: Understanding human behaviour

4: Privacy by Design

- Step 1 – Proactive, not reactive, preventative not remedial
- Step 2 – Privacy as a default setting
- Step 3 – Privacy embedded into design
- Step 4 – Full functionality
- Step 5 – End-to-end security
- Step 6 – Visibility and transparency
- Step 7 – Respect for user privacy, keep it User Centric.

(PBD Seven Steps: Reference: *Strategic Privacy by Design* by R. Jason Cronk, 2018)

Australian Government

Office of the Australian Information Commissioner

Questions

Andrew Solomon
Assistant Commissioner, Dispute Resolution

@OAICgov