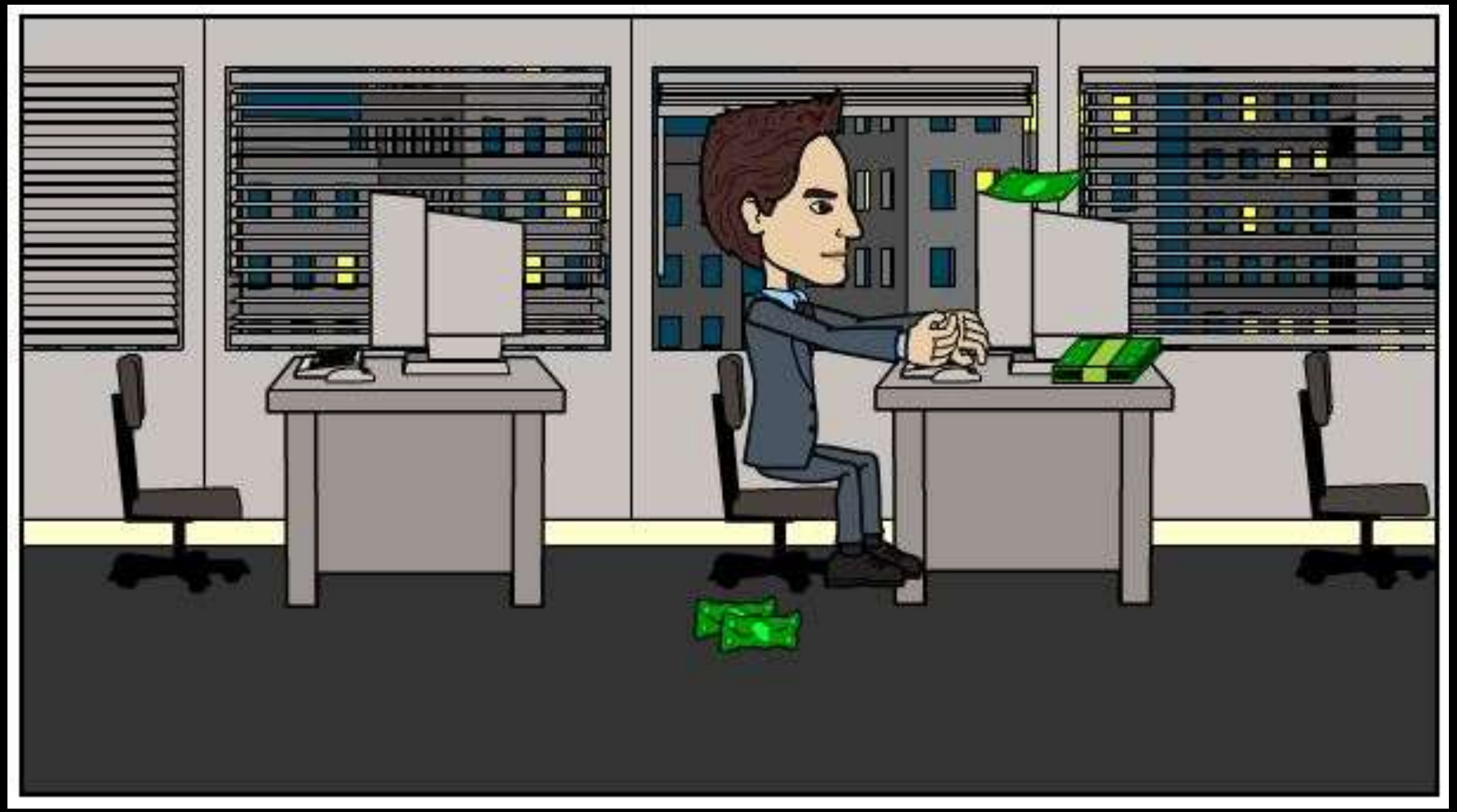
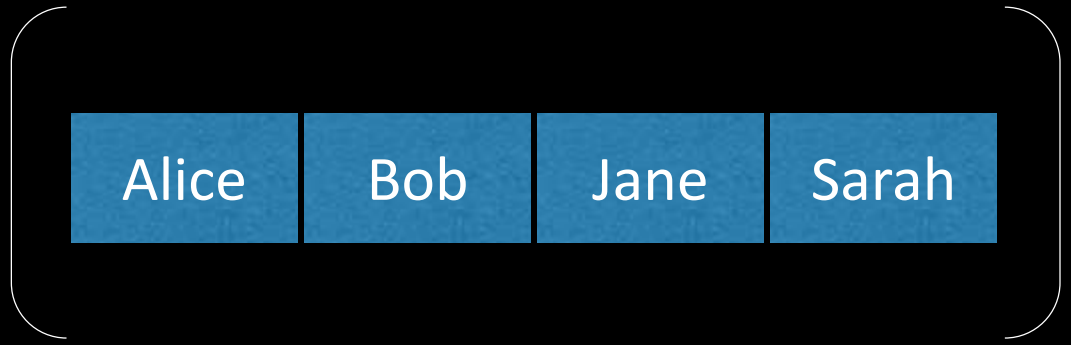
Confidential Computing: Fighting Crime & Cyber Attacks in a Privacy Preserving Way

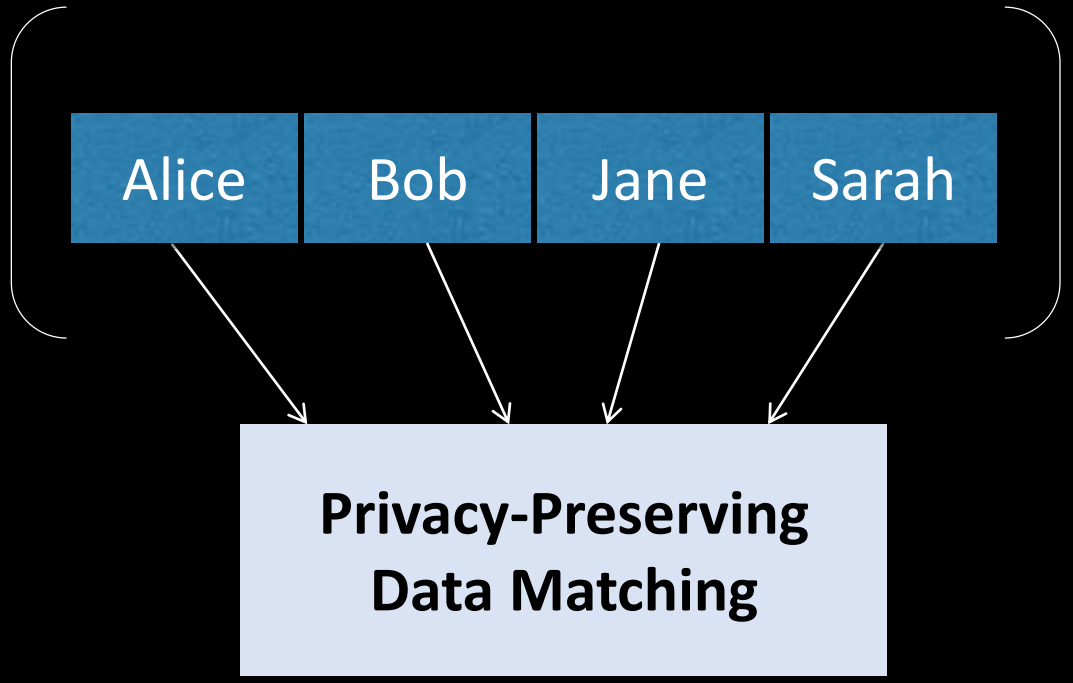
Dr. Alex Antic (ANU/AUSTRAC)



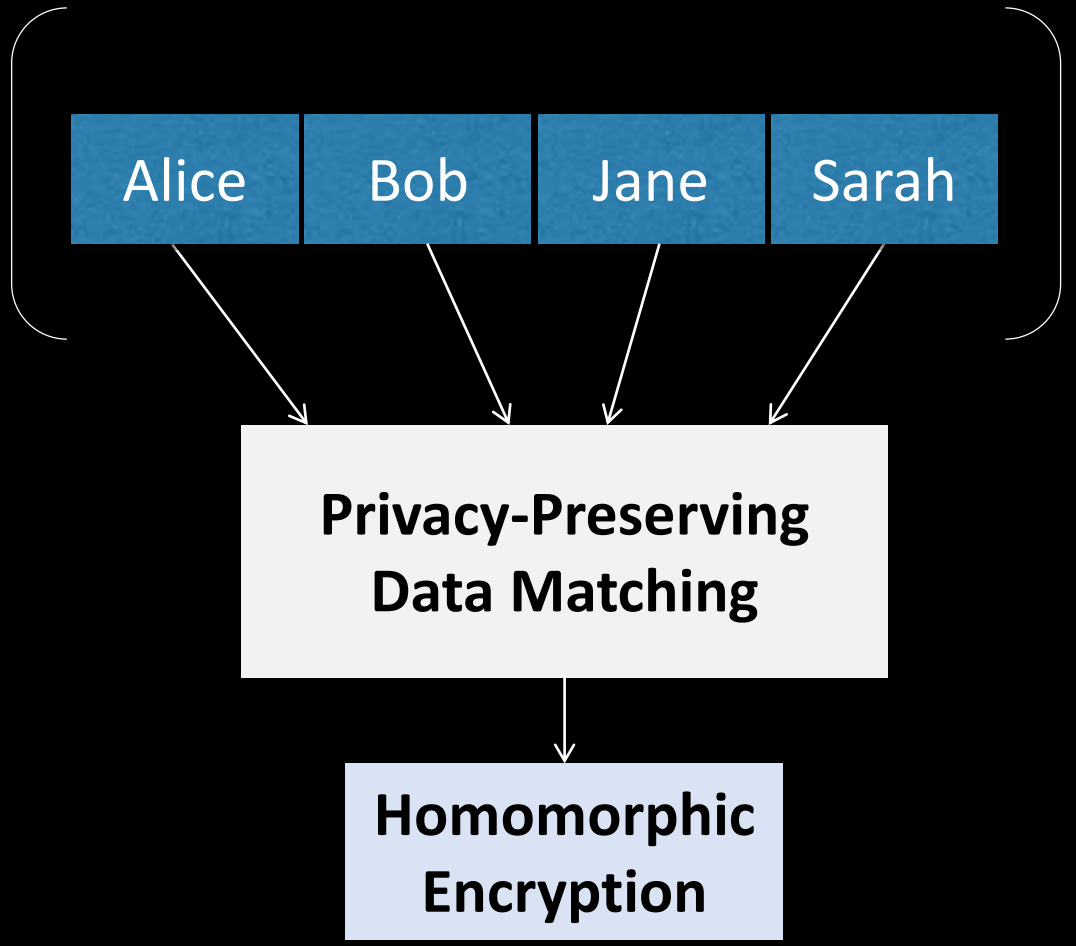
Show Me The Money!



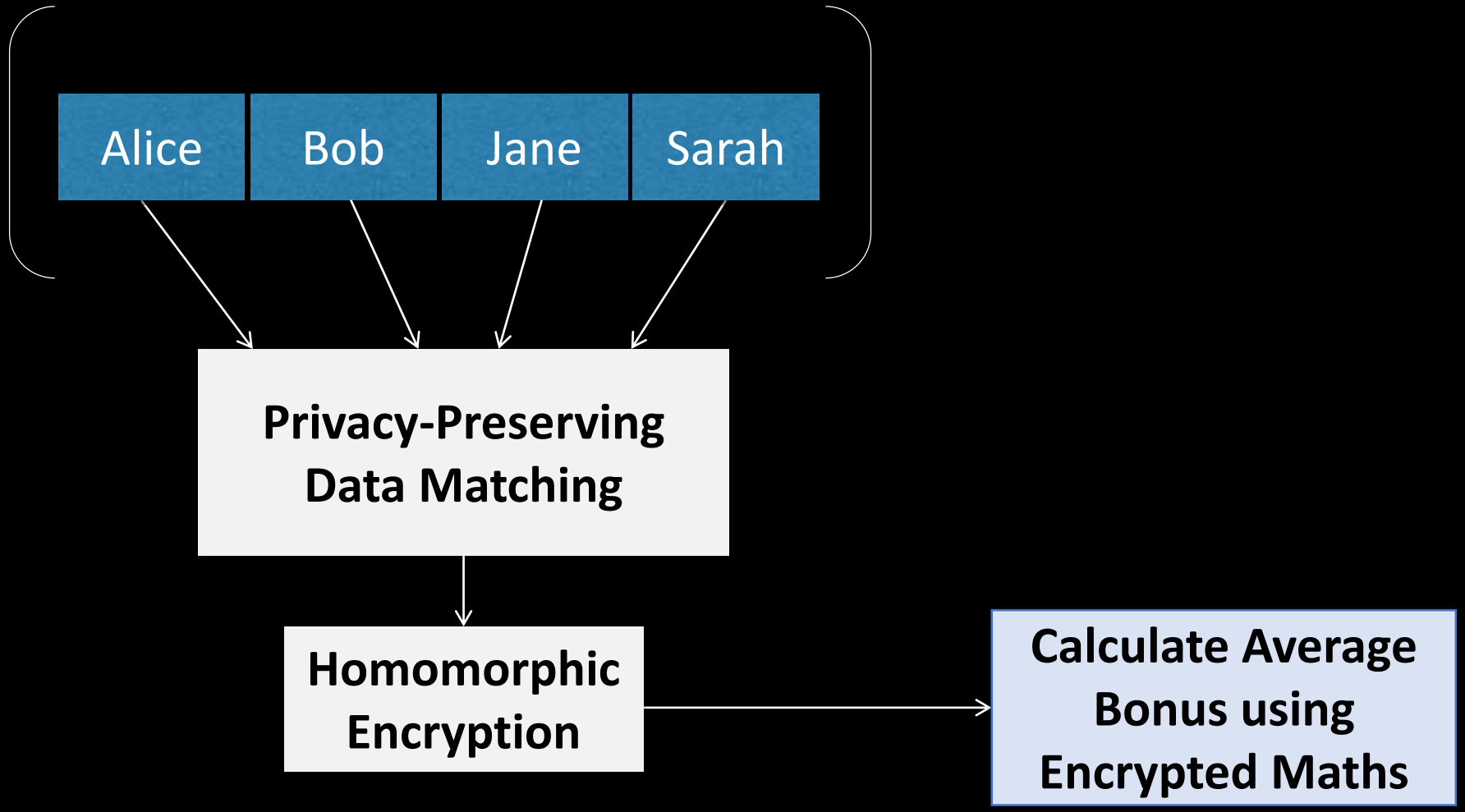
Show Me The Money!



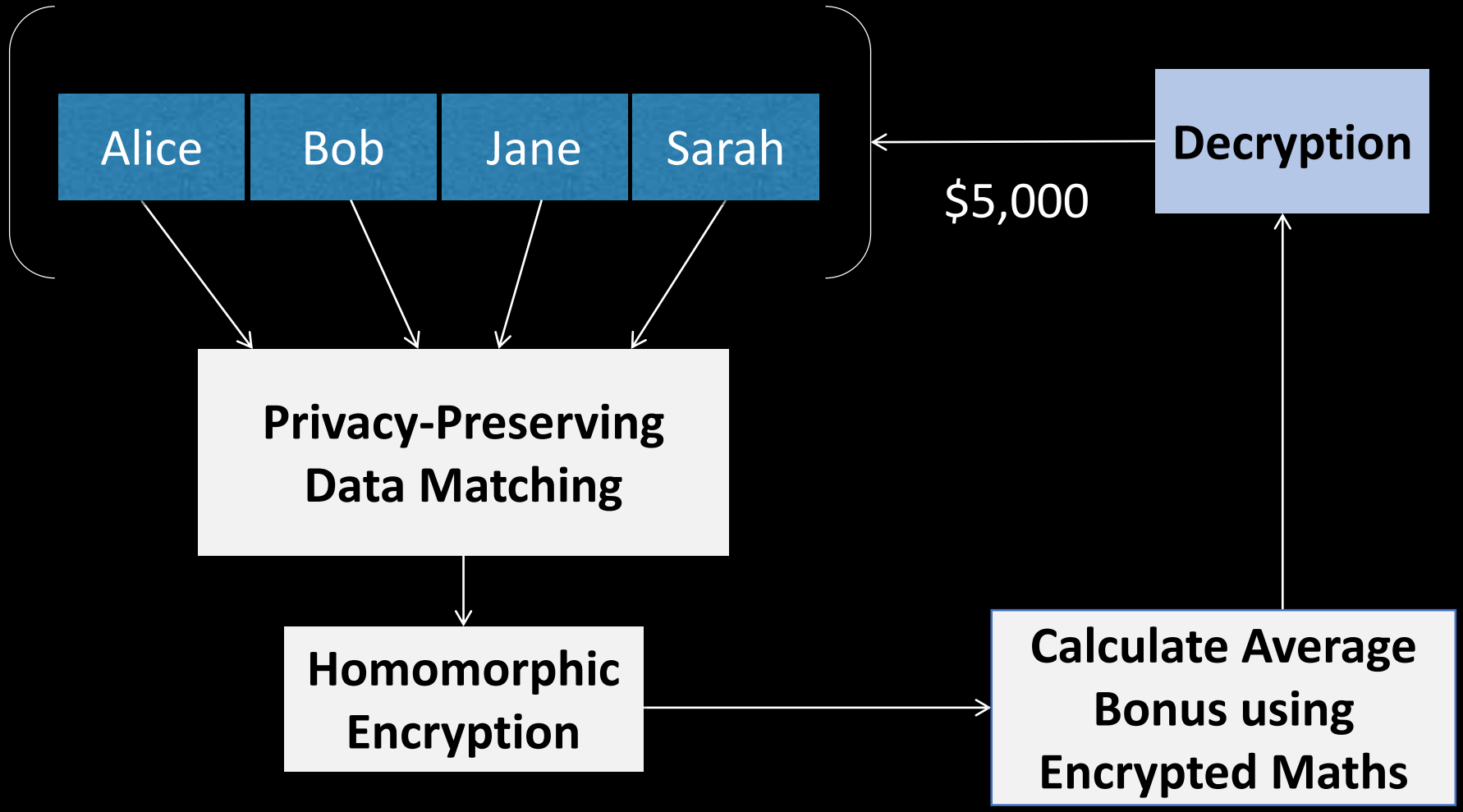
Show Me The Money!



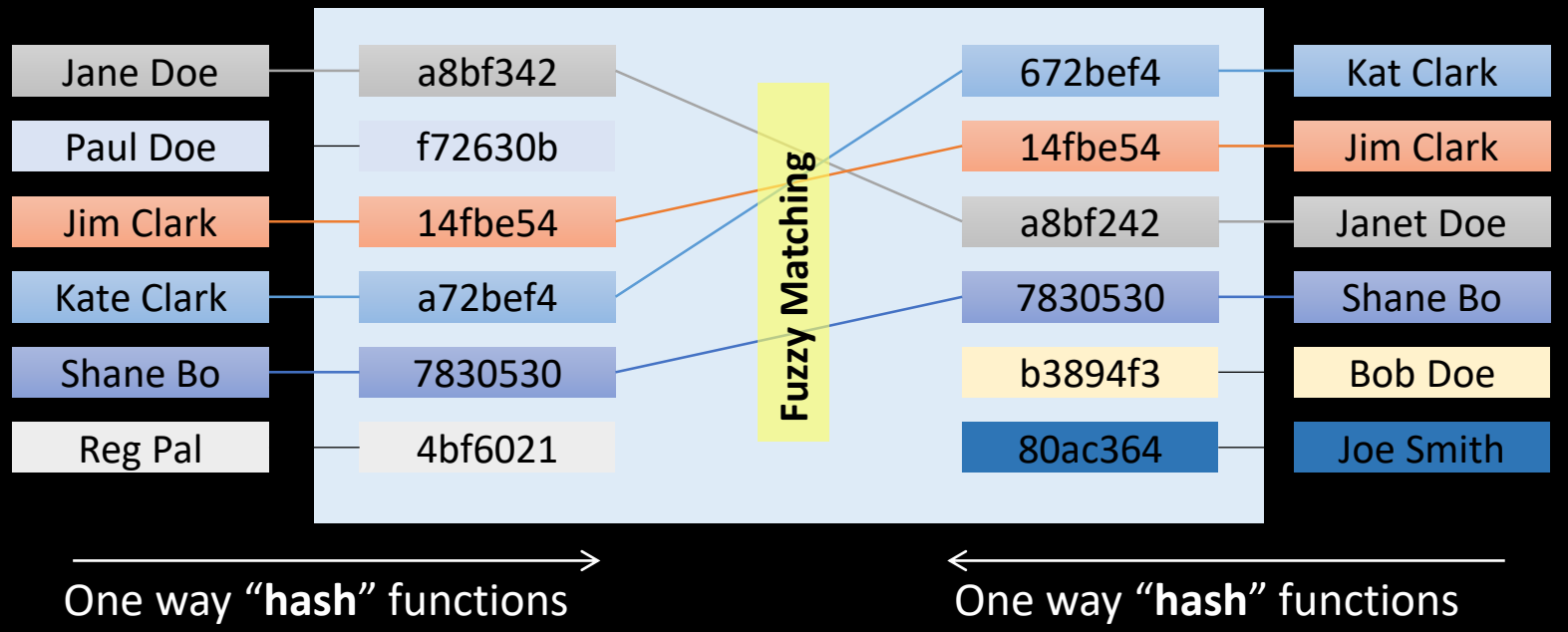
Show Me The Money!



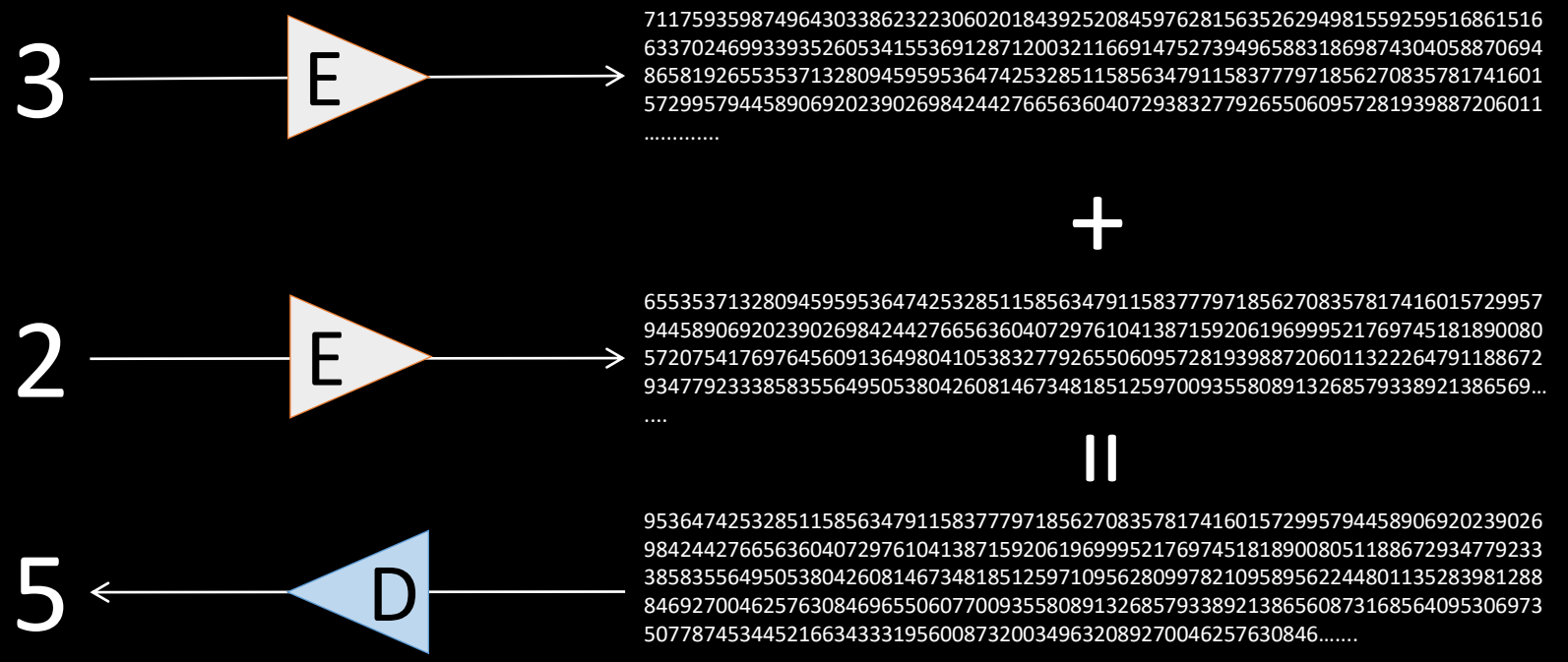
Show Me The Money!



Privacy Preserving Data Matching



Homomorphic Encryption



Individual Privacy

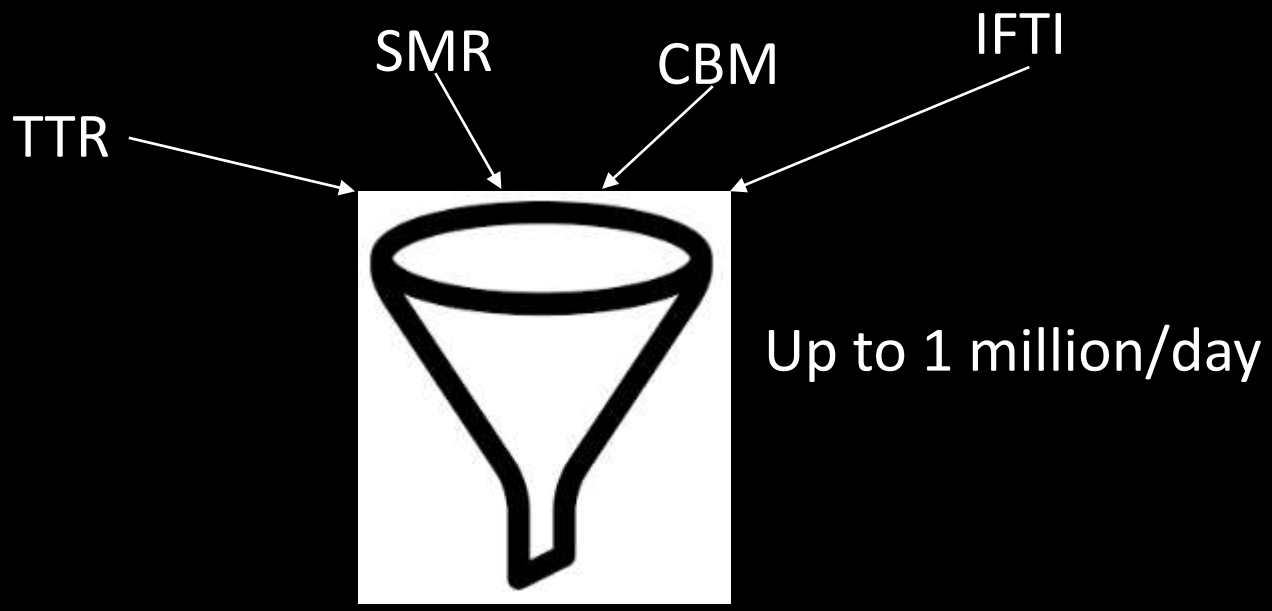
Detect. Deter. Disrupt.

$US2.5 trillion

1%

In Search of Smurfs

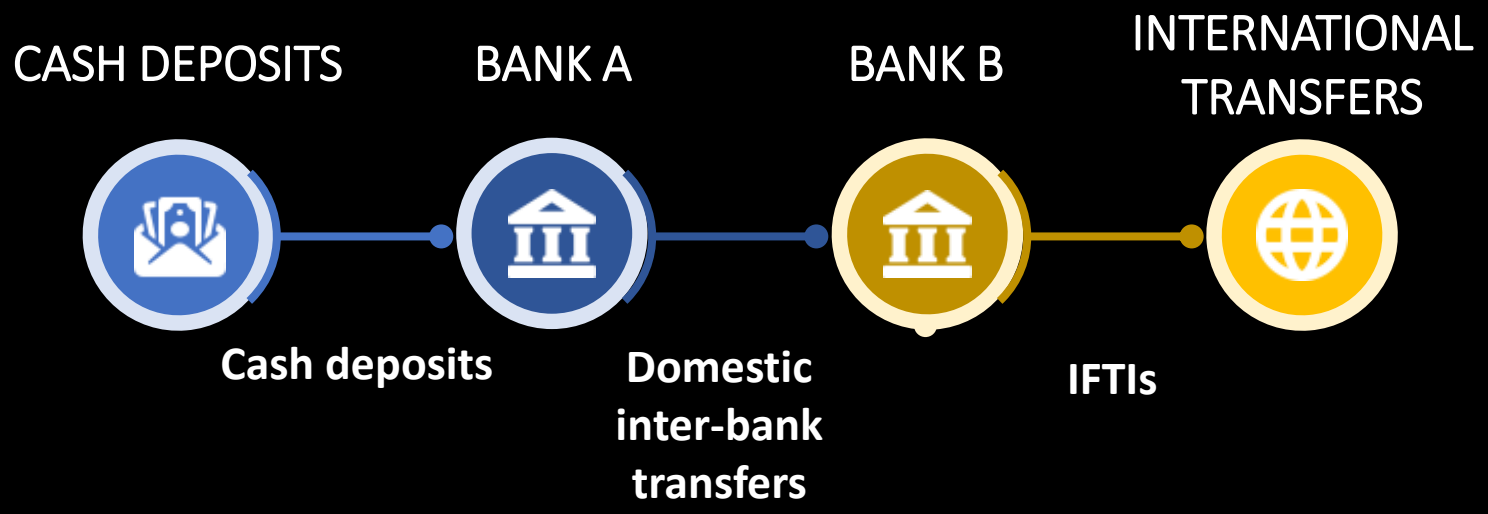
Detect, Deter & Disrupt **Money Laundering** and **Terrorism Financing**



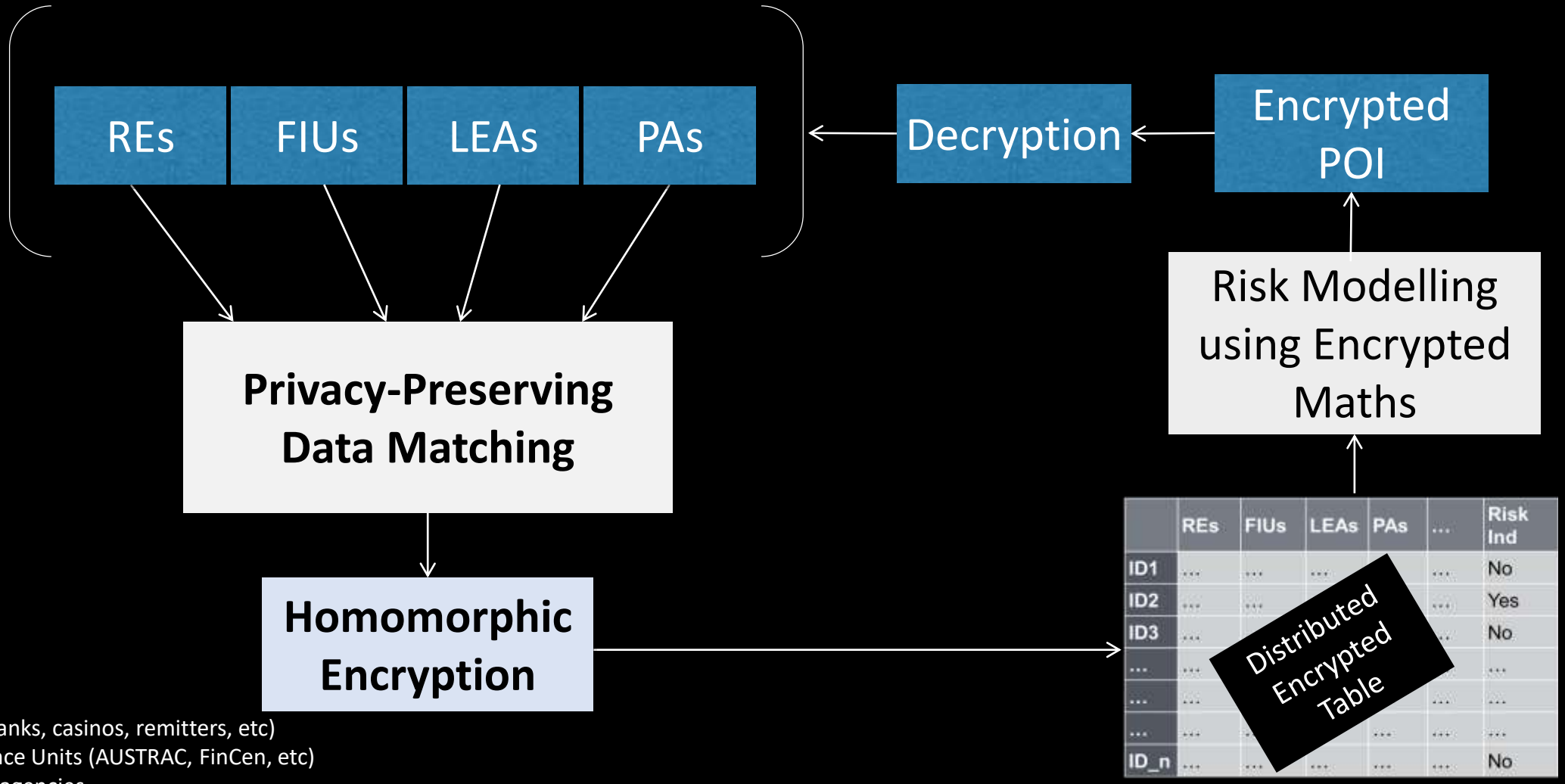
AUSTRAC

FINANCIAL INTELLIGENCE AGENCY & REGULATOR

Confidential Computing in Action



Generating Alerts (Future State)



RE = Reporting Entity (banks, casinos, remitters, etc)
FIU = Financial Intelligence Units (AUSTRAC, FinCen, etc)
LEA = Law enforcement agencies
PA = Partner agencies (e.g. ATO, DHS)

Fighting Cyber Crime

State Actors are Playing Up

Over the past 3 FY's, there were 1,097 cyber incidents affecting unclassified and classified government networks which were "considered serious enough to warrant an operational response"

Cyber attacks against Australian government infrastructure are the "new normal"

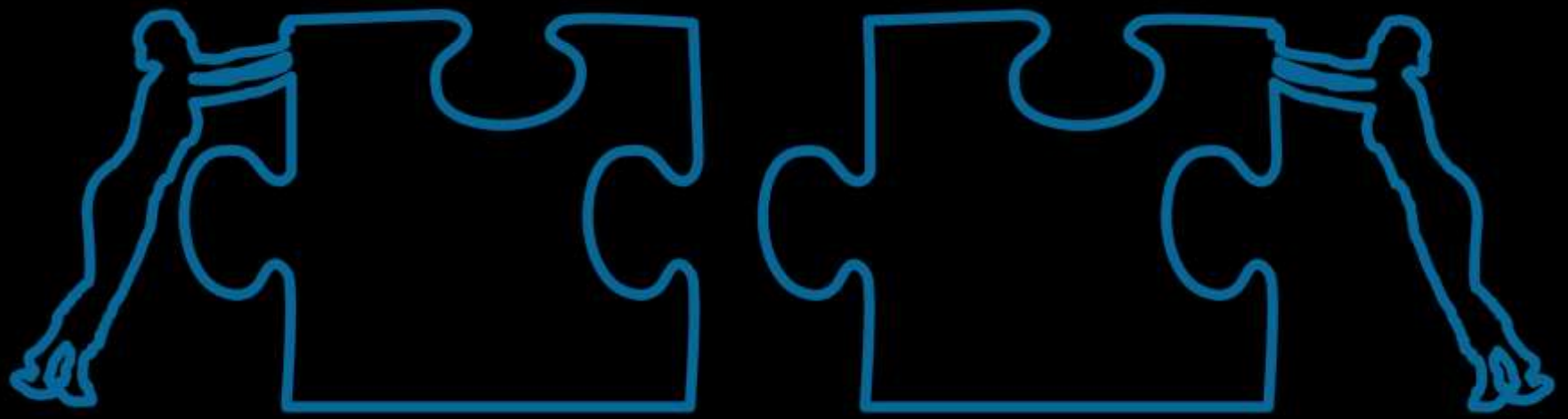
- Tom Sears (cyber defence expert)

Cyber Crime – It’s an Epidemic

Common methods used to model and analyse cyber epidemics, such as malware propagation, include susceptible-infected-susceptible (SIS)/susceptible-infected-removed (SIR)

However, privacy issues make it difficult to collect adequate data to count/estimate infected networks

Sharing is Caring…



Confidential Computing: **Analyse** & **Use** Data Without **Seeing** It

Healthcare Systems & Beyond…

"In Australian cybersecurity, there are only two types of healthcare organisations - those that **know** they've been hacked and those that **don't know** they've been hacked."

Dr Nathan Pinskier (Royal Australian College of General Practitioners & e-health specialist)

alex.antic@anu.edu.au

www.linkedin.com/in/alexantic/