RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: PRV-W02

Threat Modeling Privacy

Jonathan Fox
Director of Privacy Engineering
Cisco Corporation

Denise Schoeneich
Privacy Engineer
Intel Corporation

Jason Cronk
Privacy and Trust Consultant
Enterprise Consulting Group
@privacymaverick

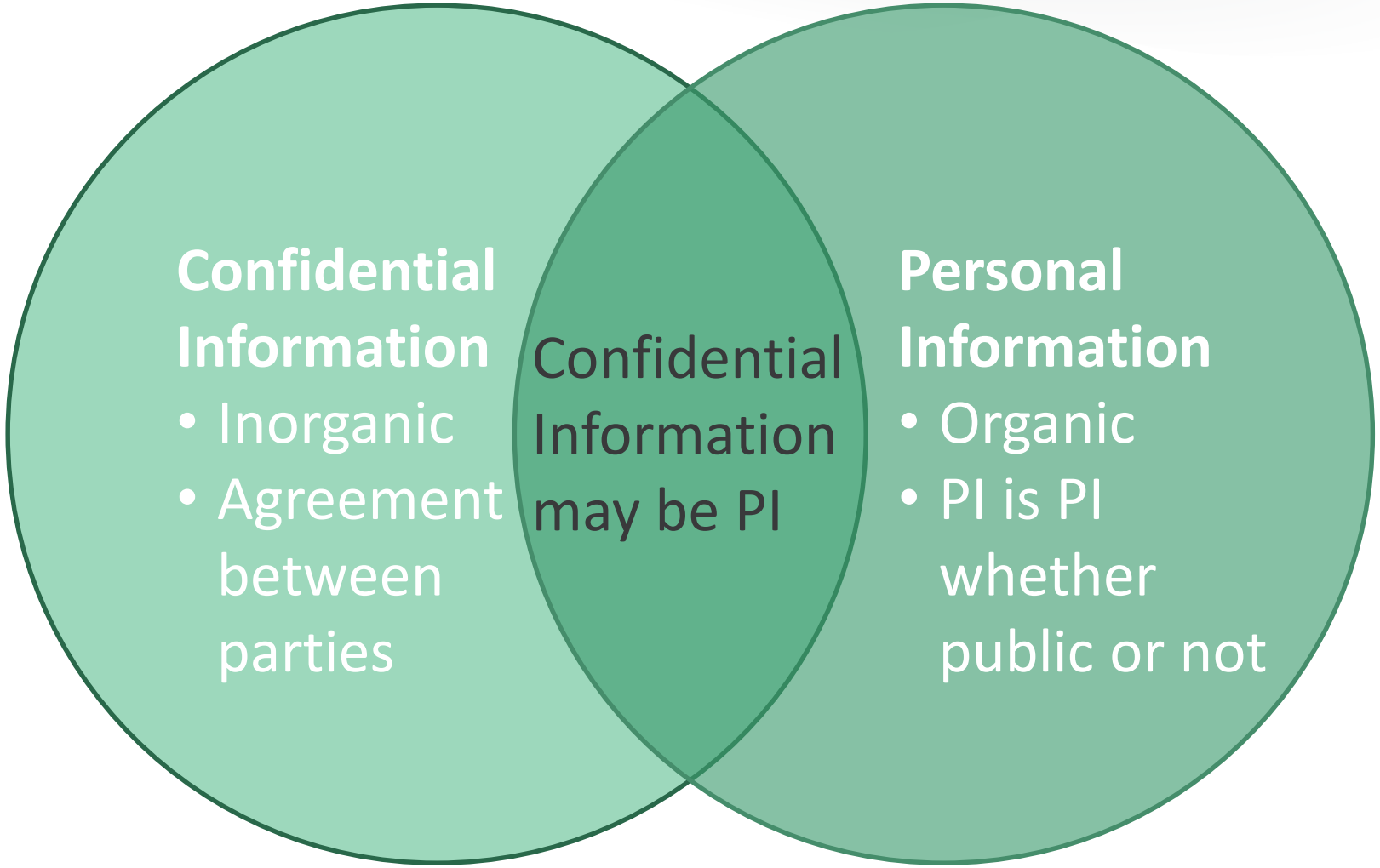
Agenda

- Privacy in Context
- Privacy Engineering
- Secure Development Lifecycle (SDL)
- Privacy Threat Modeling
- Privacy Context Diagram
- Privacy Requirements & Validation
- Hands-on Exercise

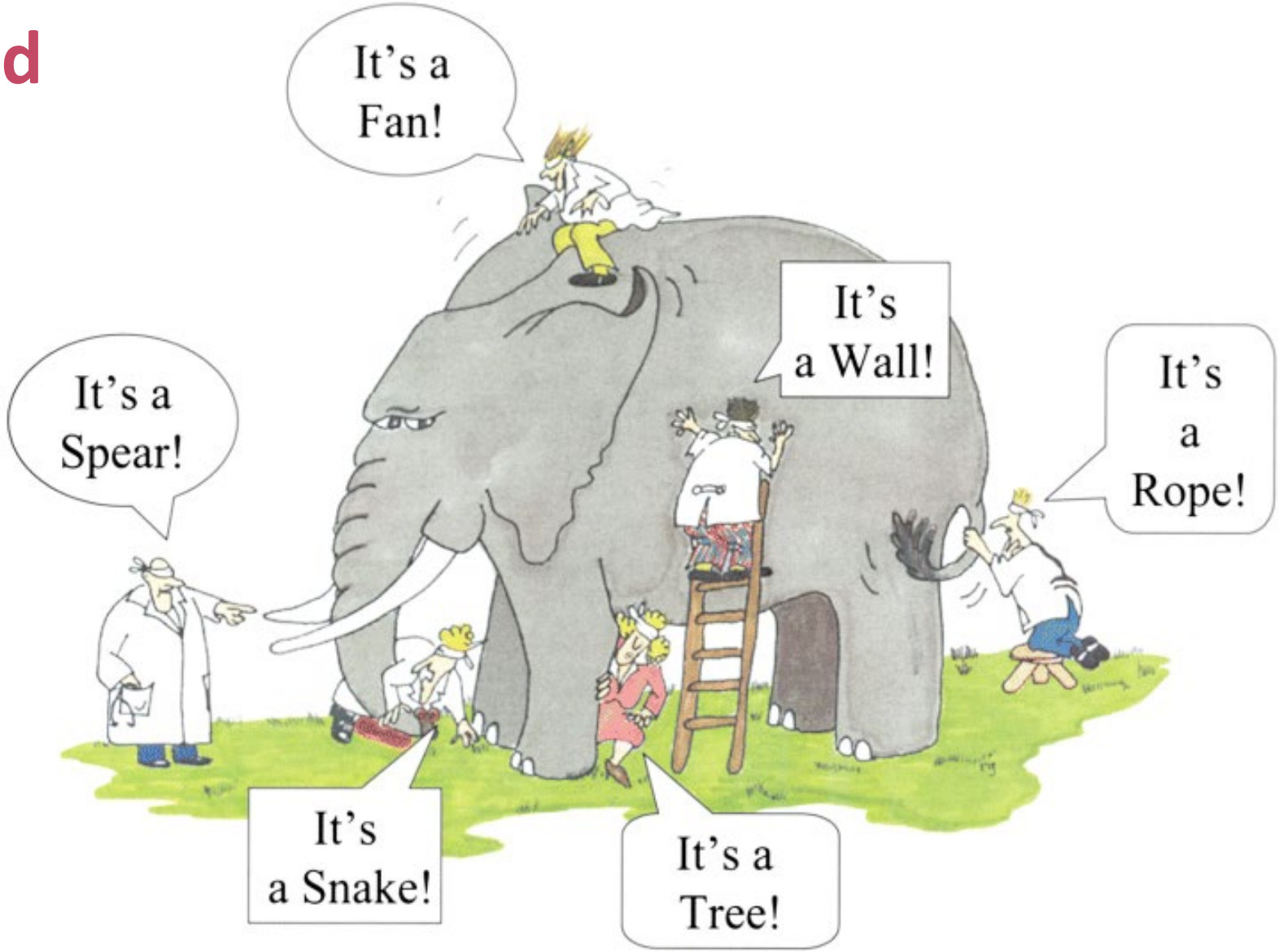
RSAConference2020

Privacy in Context

Confidential Information vs. Personal information



Privacy can't be fixed



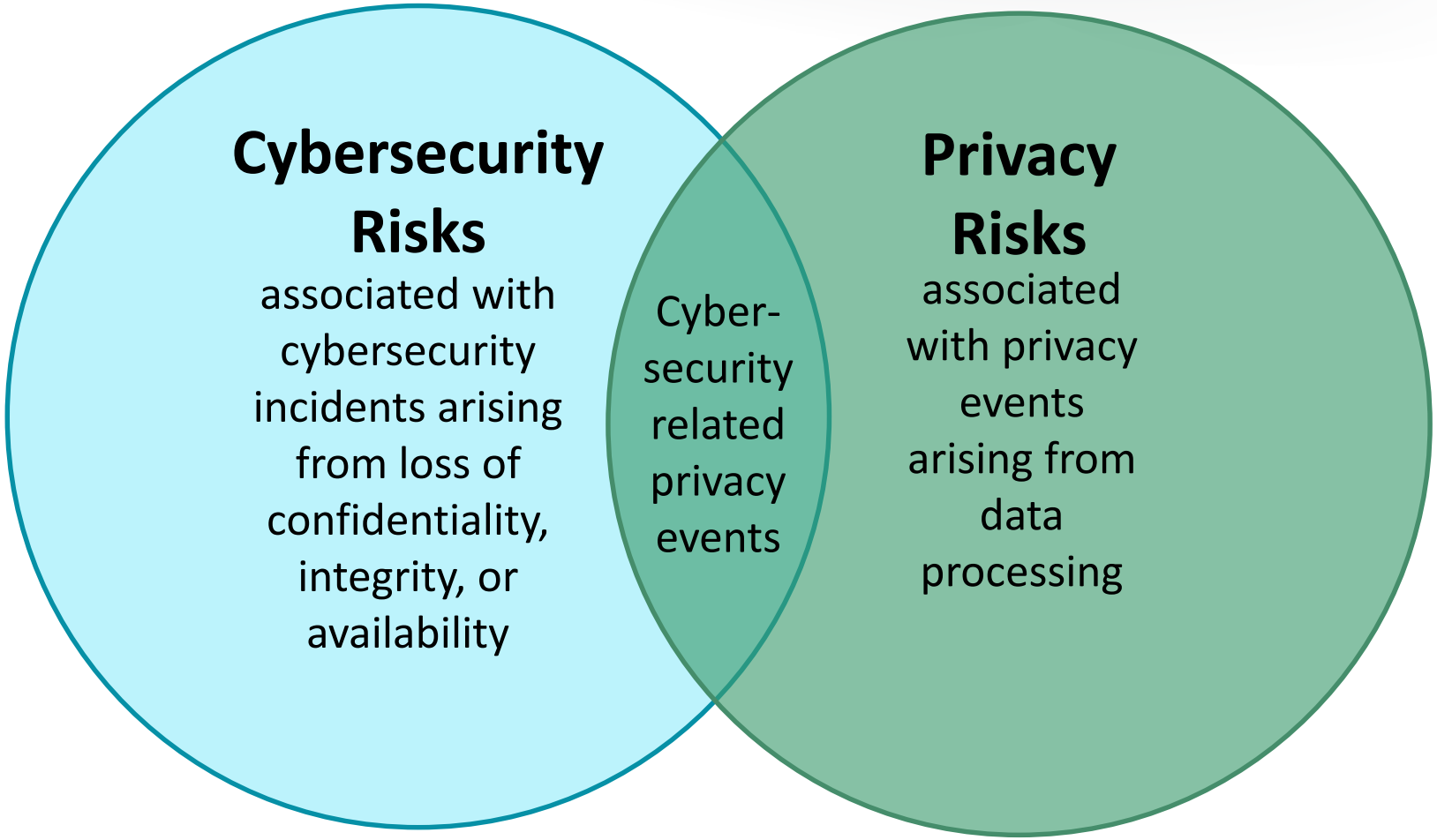
But that doesn't mean
It's broken

It’s a balancing act

- Rights of the individual
- Rights of the Organization

- Obligations of the individual
- Obligations of the Organization

The overlap between privacy and security risks



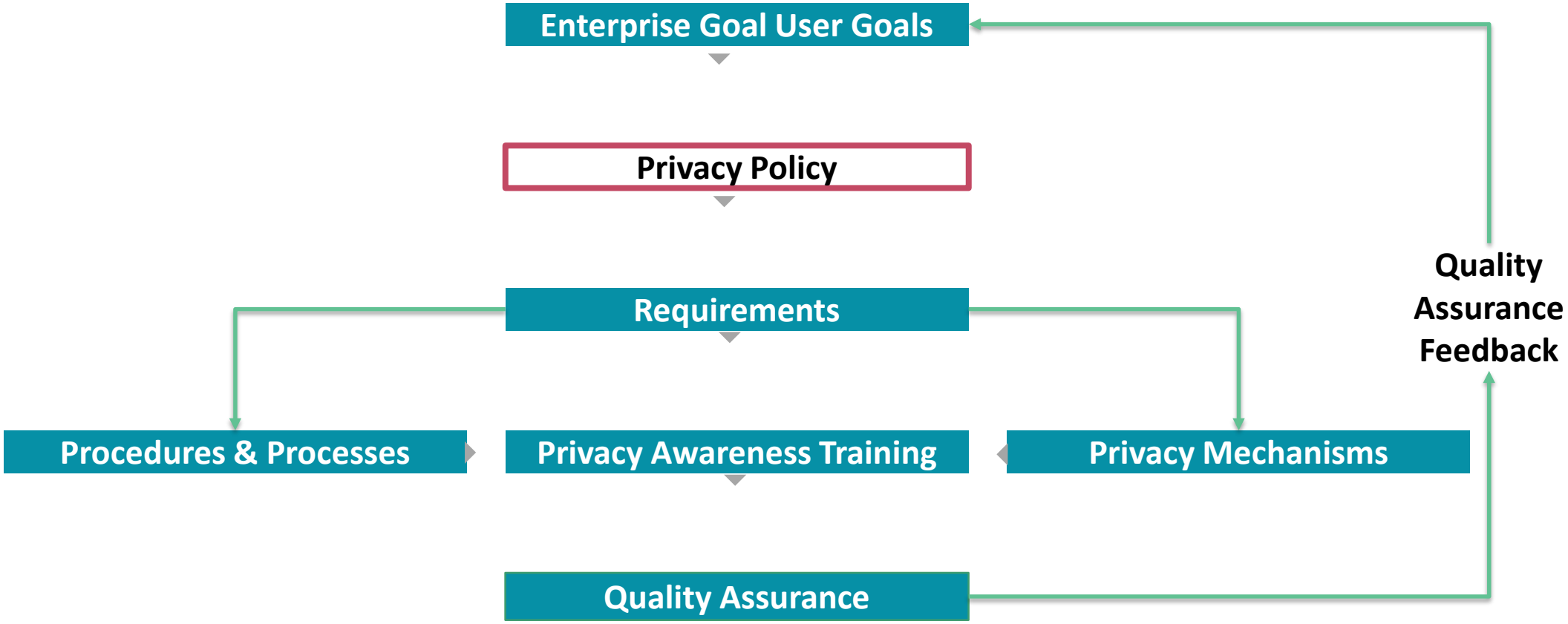
https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf. February 10, 2020

RSAConference2020

Privacy Engineering

Requirements Cross Multiple Layers…

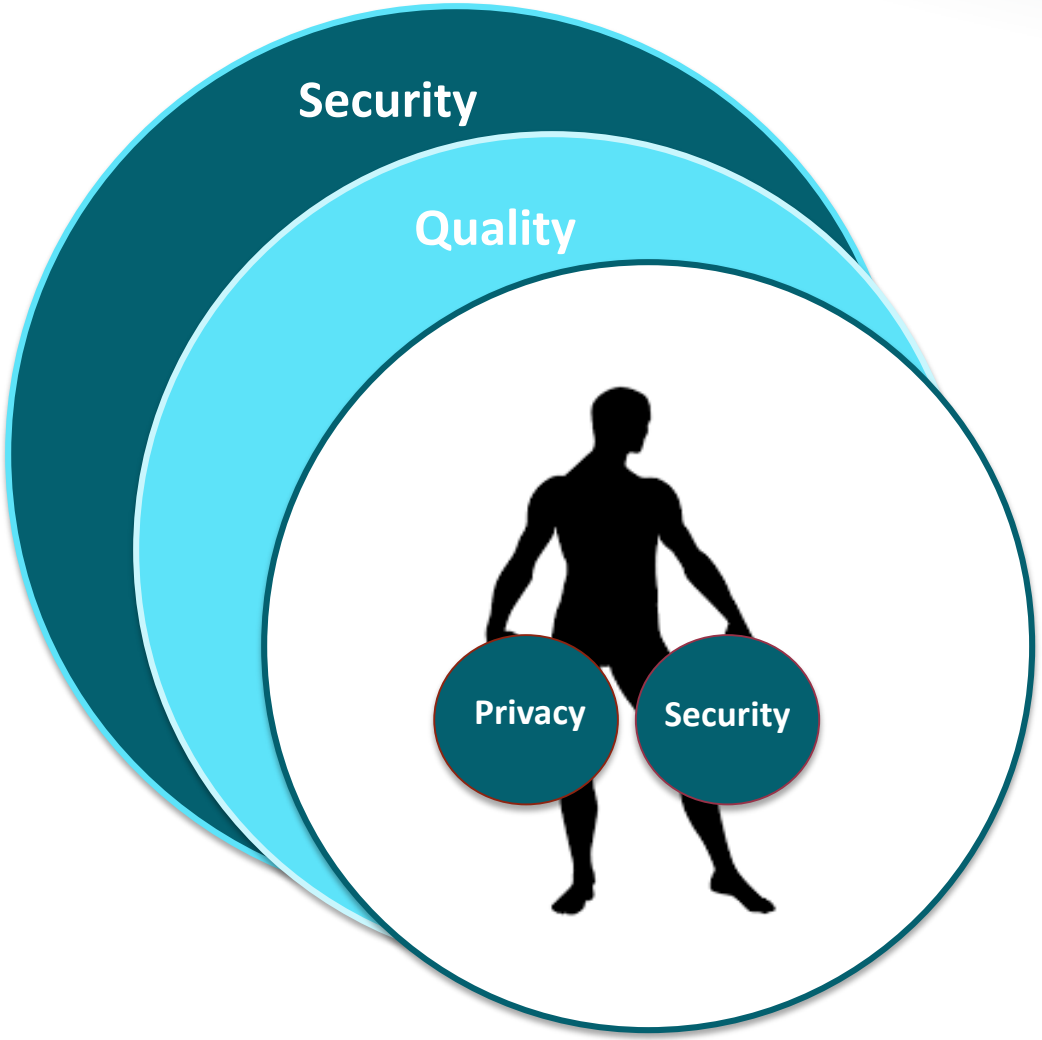
Privacy Engineering Development Process



RSAConference2020

Secure Development Lifecycle (SDL)

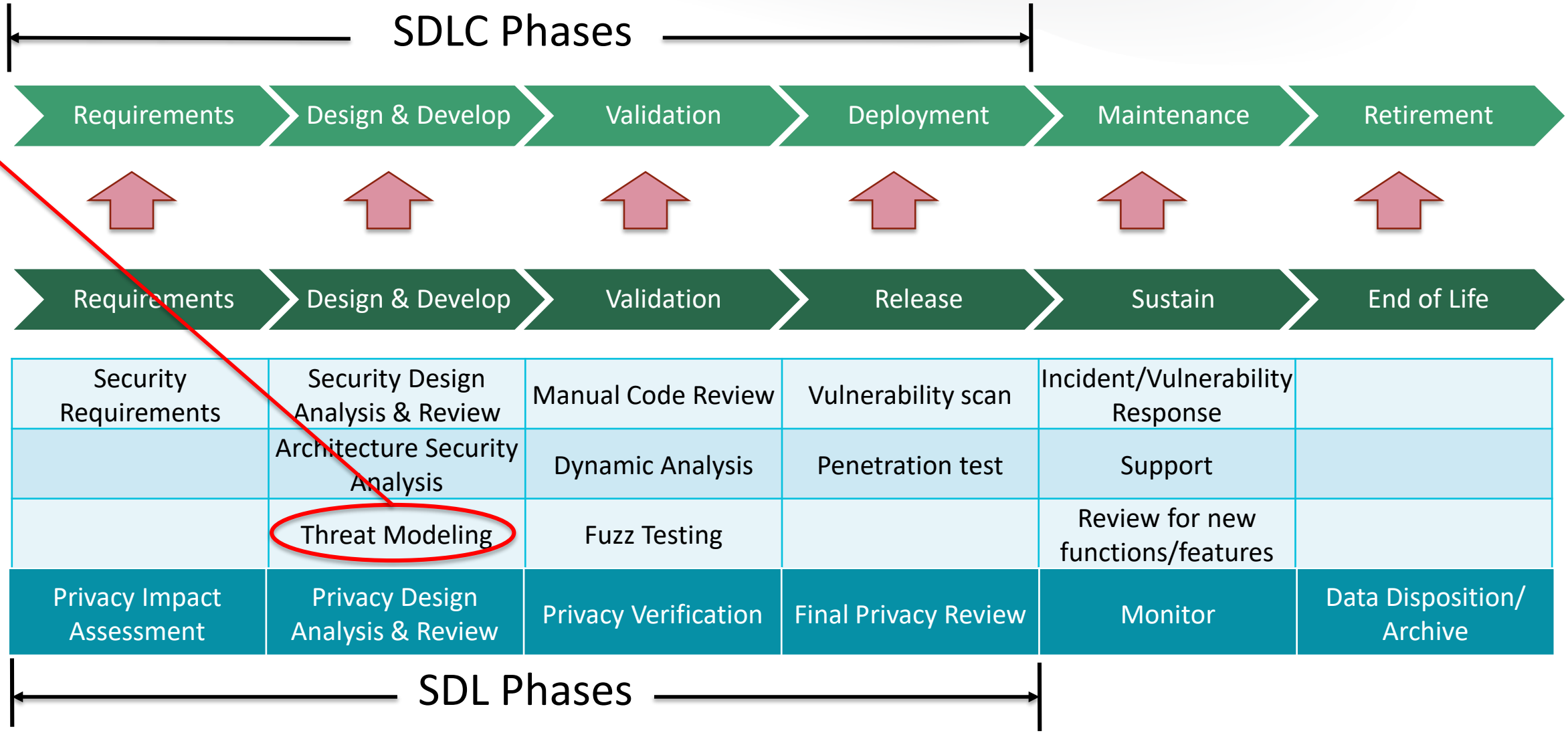
Privacy Engineering Requires Both Quality and Security



SDLC/SDL

Privacy Impact Assessment

Secure Development Lifecycle (SDL) Mapped to the SDLC



RSAConference2020

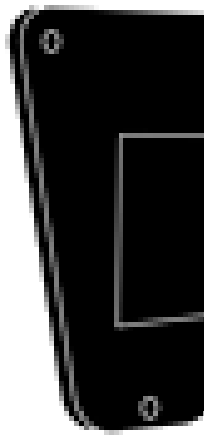
Privacy Threat Modeling

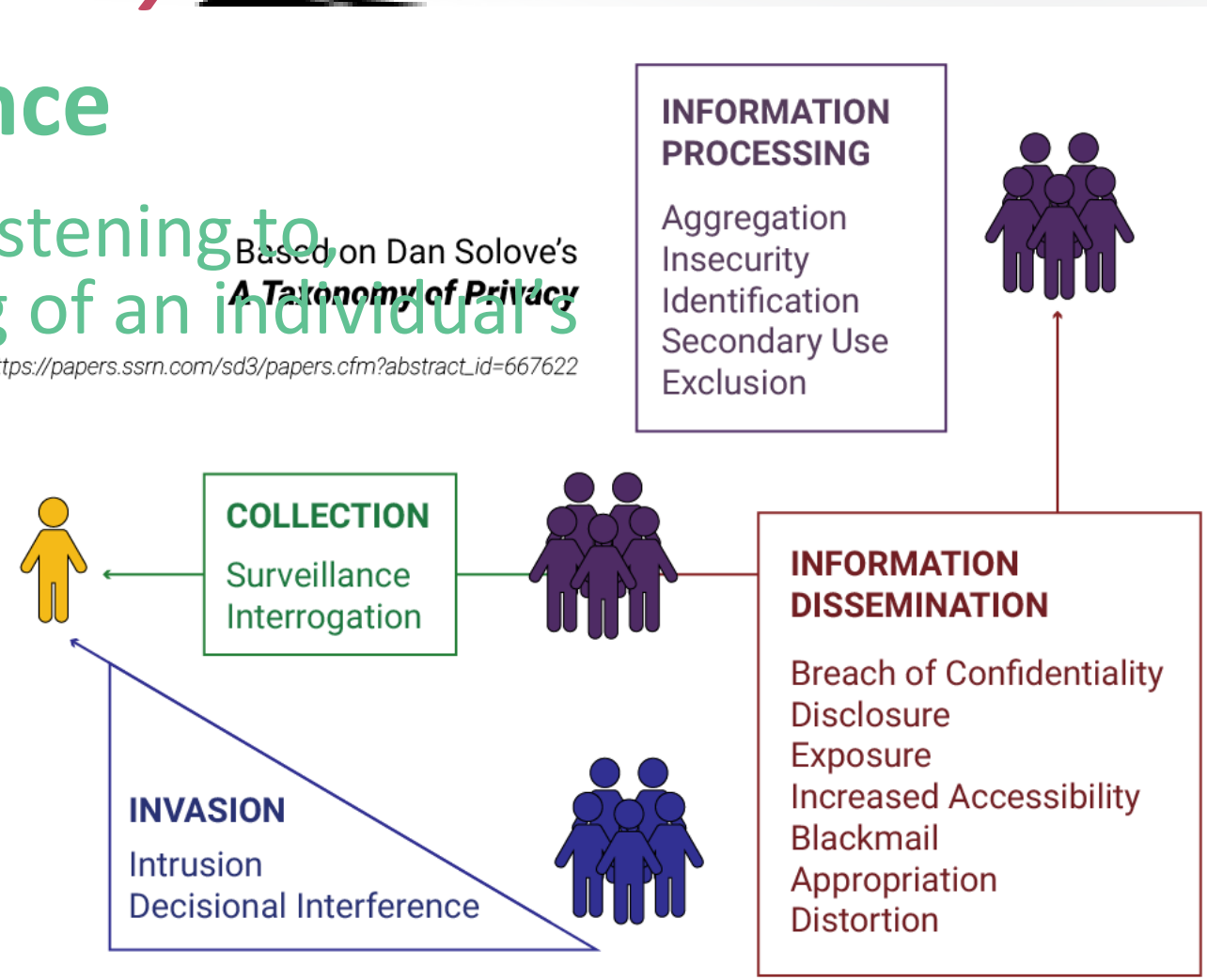
Privacy Threat Modeling
What is *privacy*?

Surveillance

Watching, listening to, or recording of an individual's activities.

Based on Dan Solove's
A Taxonomy of Privacy
https://papers.ssrn.com/sd3/papers.cfm?abstract_id=667622





Privacy *Threat* Modeling
What is a *threat*?

Is a bald tire a threat?

Threat

car loses traction

swing breaks

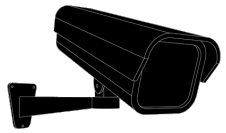
Bald tire is a ~~Vulnerability~~

Credit for example: Jack Jones of FAIR Institute

Risk

RISK = Likelihood of threat exploiting a vulnerability and severity of resulting consequences

(Threats | Vulnerabilities | Consequences) → RISK



Install a camera | Unlocked door | Surveillance & Embarrassment

← Primary

← Secondary

Privacy Controls

NIST SP 800-53 Families

- Authority and Purpose
- Accountability, Audit and Risk Management
- Data Quality and Integrity
- Data Minimization and Retention
- Individual Participation and Redress
- Security
- Transparency
- Use Limitation

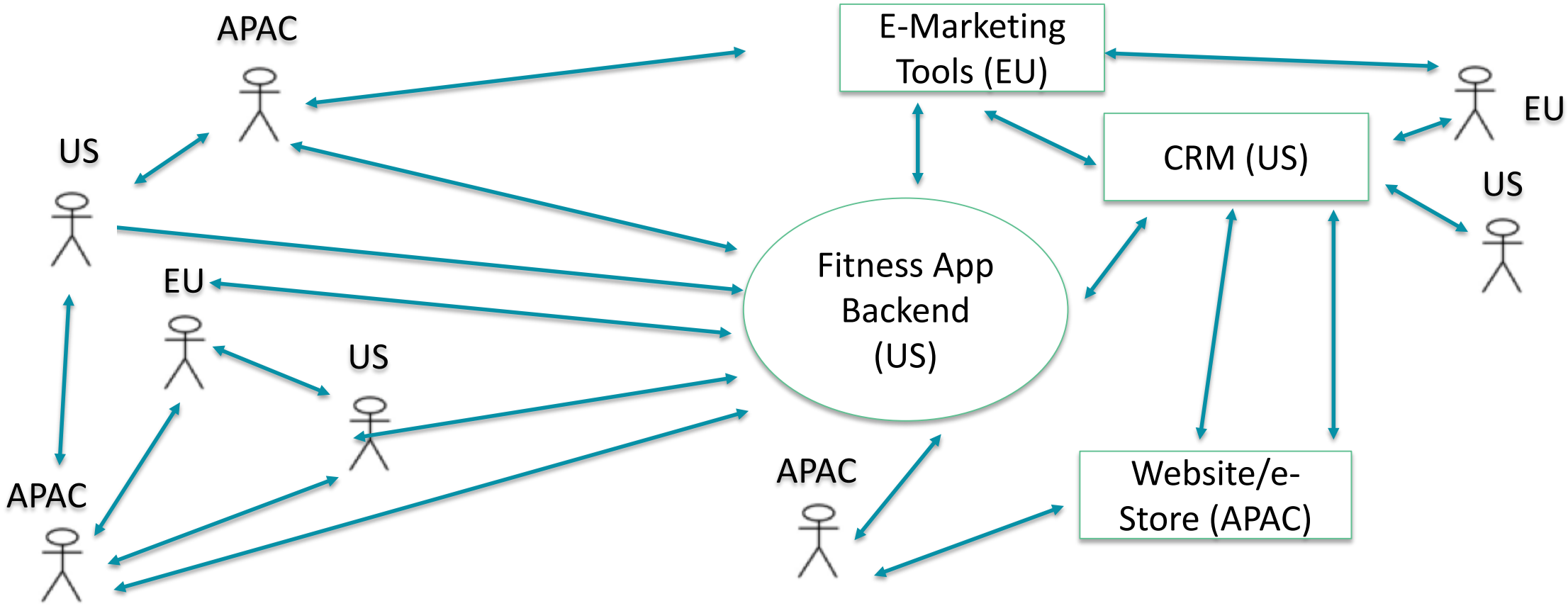
Hoepman Privacy Design Strategies

- MINIMIZE
- SEPARATE
- ABSTRACT
- HIDE
- ENFORCE
- DEMONSTRATE
- INFORM
- CONTROL

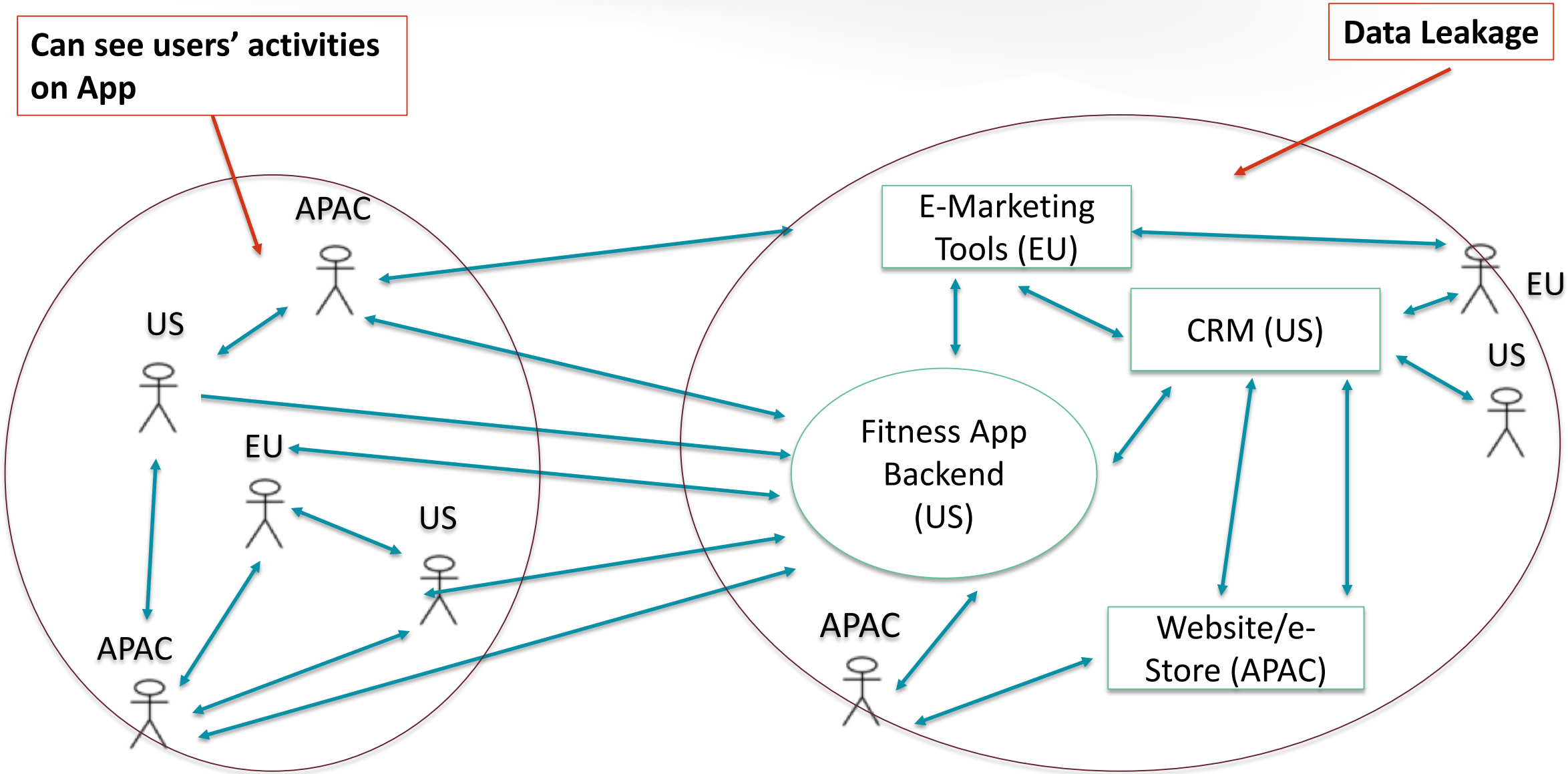
RSAConference2020

Privacy Context Diagram

Build of a Context Diagram



Layer in Threats



RSAConference2020

Hands-on Exercise

Threat Model CHARETTE

Scenario

Shop til' you drop

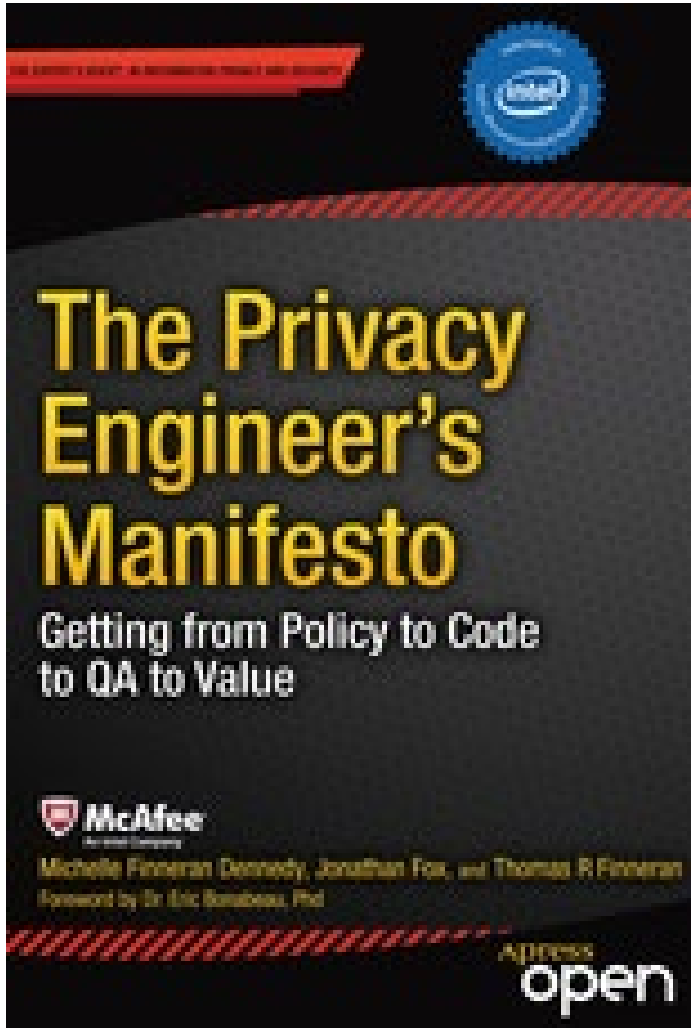
Design a supermarket app that creates shopping lists based on shopping history, maps user's path in the store, and directs user to bargains (i.e., ties into supermarket's affinity program).

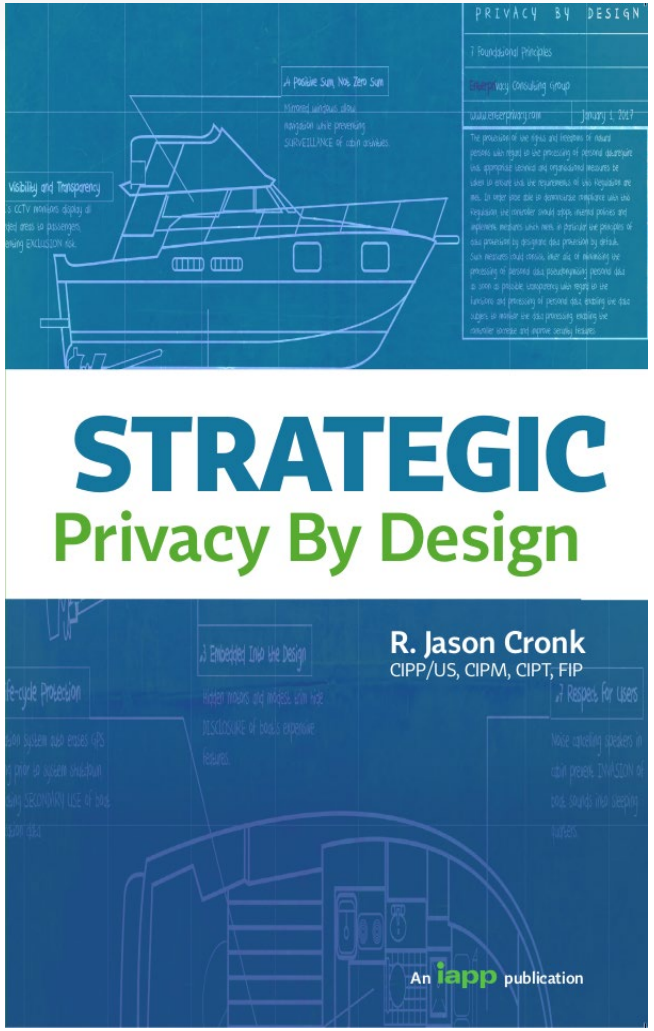
- Identify three possible threats
- Identify possible consequences to the individual
  - Consider both primary and secondary
- Identify controls to mitigate the risk

Note: Business model is advertising and data monetization

Apply What You Have Learned Today

- Next Week you should:
  - Review your Secure Development Lifecycle (SDL) for gaps in how privacy is incorporated
- In the first three months following this presentation you should:
  - Begin to fill identified gaps
- Within six months you should:
  - Select a development project and create a context diagram with privacy data flows, uses, interactions, threats and controls


The Privacy Engineer's Manifesto
Getting from Policy to Code to QA to Value
McAfee
Michelle Finneran Dennedy, Jonathan Fox, and Thomas R Finneran
Foreword by Dr. Eric Bonabeau, PhD
Apress
open


PRIVACY BY DESIGN
STRATEGIC
Privacy By Design
R. Jason Cronk
CIPP/US, CIPM, CIPT, FIP
An iapp publication

Resources

- Annex Guide to Privacy by Design Privacy by Design Documentation for Software Engineers Version 1.0 (OASIS)
- Architecture of Privacy (O'Reilly Media)
- Core Software Security: Security at the Source (CRC Press)
- Linddun Privacy Threat Modeling (LINDDUN)
- NIST Privacy Framework 1.0 (NIST)
- P7002 - Data Privacy Process (IEEE Standards Association) - Under development
- ISO/PC 317- Consumer protection: privacy by design for consumer goods and services – Under development
- Privacy and Data Protection by Design (ENISA)
- Privacy Design Strategies (Institute for Computing and Information Sciences)
- Privacy Engineering, A Data Flow and Ontological Approach (CreateSpace)
- Privacy Engineering & Assurance (IAPP)
- Privacy Engineer's Manifesto (Apress)
- Strategic Privacy by Design (IAPP)
- Taxonomy of Privacy (University of Pennsylvania Law Review)