October 16, 2019

Dynamic Duo – Privacy Threat Modeling and Context Diagramming in the SDLC

Denise Schoeneich
Intel Corporation

Jonathan Fox
Cisco Corporation

Jason Cronk
Privacy and Trust Consultant Enterprise Consulting Group

Privacy+ Security Forum

Speaker

Denise Schoeneich
Privacy Engineer
Intel Corporation

Denise is responsible to ensure appropriate and timely privacy solutions are engineered into the AI data lifecycle.
IAPP FIP, CIPP/US, CIPT, CIPM

Speaker

Privacy+ Security Forum

Jonathan Fox

Director, Privacy Engineering

Cisco Corporation

Jonathan is a member of Cisco's Chief Privacy Office and co-author of the upcoming The Privacy Engineer's Companion: A Workbook of Guidance, Tools, Methodologies, and Templates.

Speaker

Jason Cronk
Privacy and Trust Consultant
Enterprise Consulting Group

Author, Strategic Privacy by Design
Licensed Attorney in Florida, PbD Ambassador,
IAPP FIP, CIPP/US, CIPT, CIPM

Dynamic Duo – Privacy Threat Modeling and Context Diagramming in the SDLC

Privacy+ Security Forum

- **Purpose of Session**

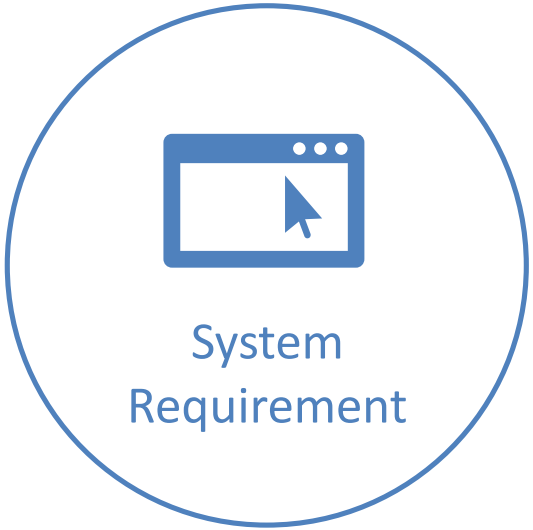
  Privacy by Design (PbD) prioritizes privacy in the initial design stages and throughout the development lifecycle. Privacy threat modeling and context diagramming can be used as an approach to implement PbD in the SDLC.

- **Main Sections**
  - Privacy Engineering
  - Secure Development Lifecycle (SDL)
  - Privacy Threat Modeling
  - Privacy Context Diagram
  - Privacy Requirements & Validation
- **Invite Questions**

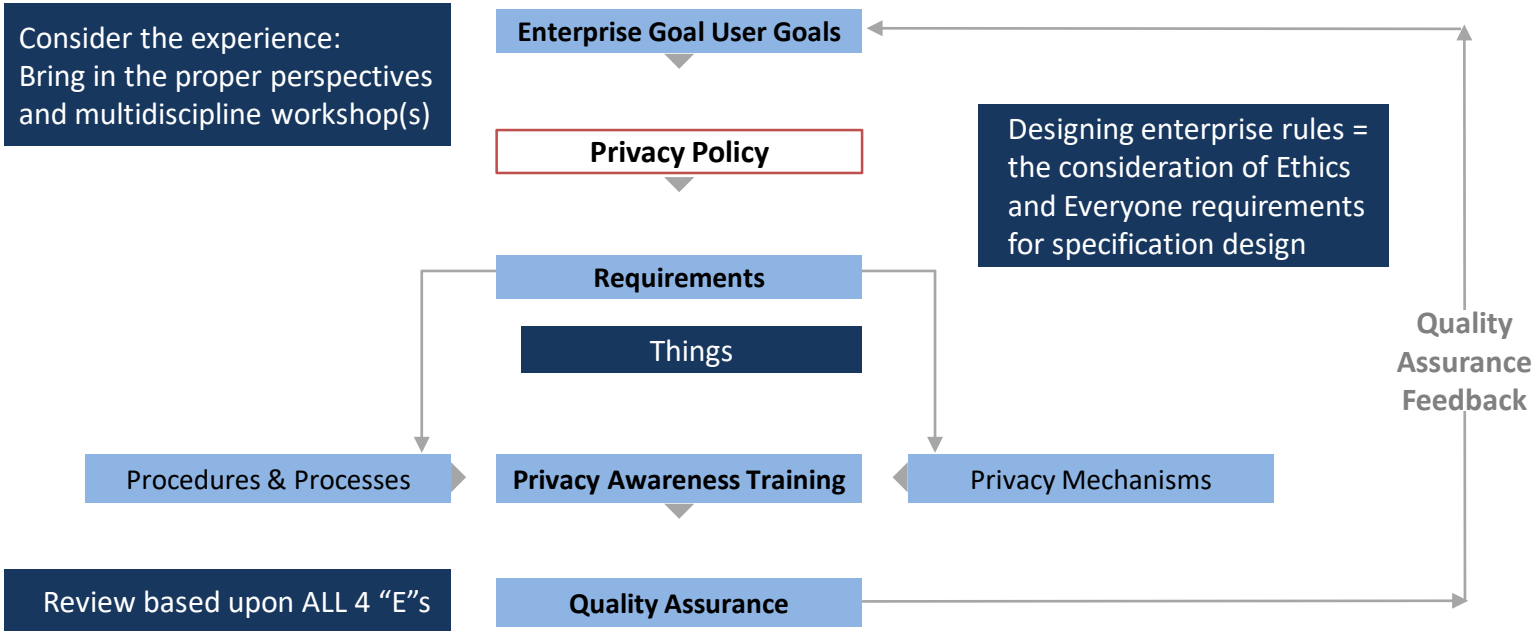
Privacy Engineering

Overview of privacy engineering including privacy engineering development process

Requirements cross multiple layers…



Privacy Engineering Development Process



Secure Development Lifecycle (SDL)

Relationship of privacy, security and quality and SDL mapped to the SDLC

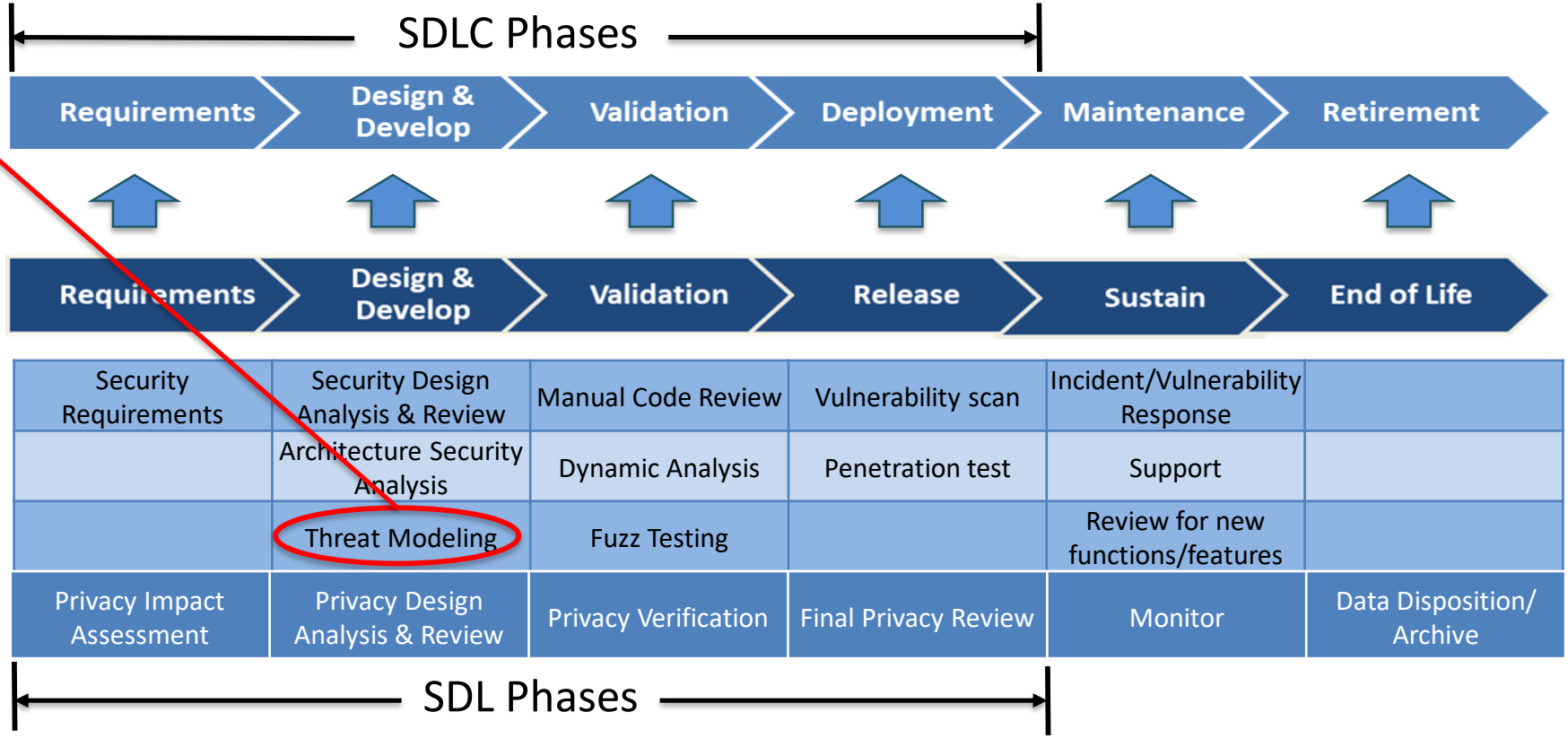
Privacy+ Security Forum

Privacy Engineering Requires Both Quality and Security

SDLC/SDL

Privacy Impact Assessment

Secure Development Lifecycle (SDL) Mapped to the SDLC



Privacy Threat Modeling

How threats pose risk to privacy, who are threat actors in a privacy context, and frameworks for modeling privacy risks

What is a threat?

Is a bald tire a threat?

Threat

- car looses traction
- swing breaks

Bald tire is a ~~Vulnerability~~

How Threats Impose Risk

(Threats Vulnerabilities Consequences) → **RISK**

Likelihood of threat exploiting a vulnerability and severity of resulting consequences

Threat Actors

	Persons	Organizations	Governments
Motivation	*Revenge, money, spite, curiosity, & control.*	*Money & competitive advantage.*	*Law enforcement, espionage, control & repression.*
Rank (skills & resources)	Solo		
	Amateur	Small	Local
	Professional	Medium	Regional
	Organized criminal	Large	Nation-state
	Crowds/mobs	Multi-national	Industrialized
		FAMGA	Superpower

Compliance Model

Most compliance models presume a certain type of threat actor

- External to the organization

- Contrary to the organization's interests

- Some include the organization (FCRA, GDPR, CAN-SPAM)

Different Frameworks for Modeling Privacy

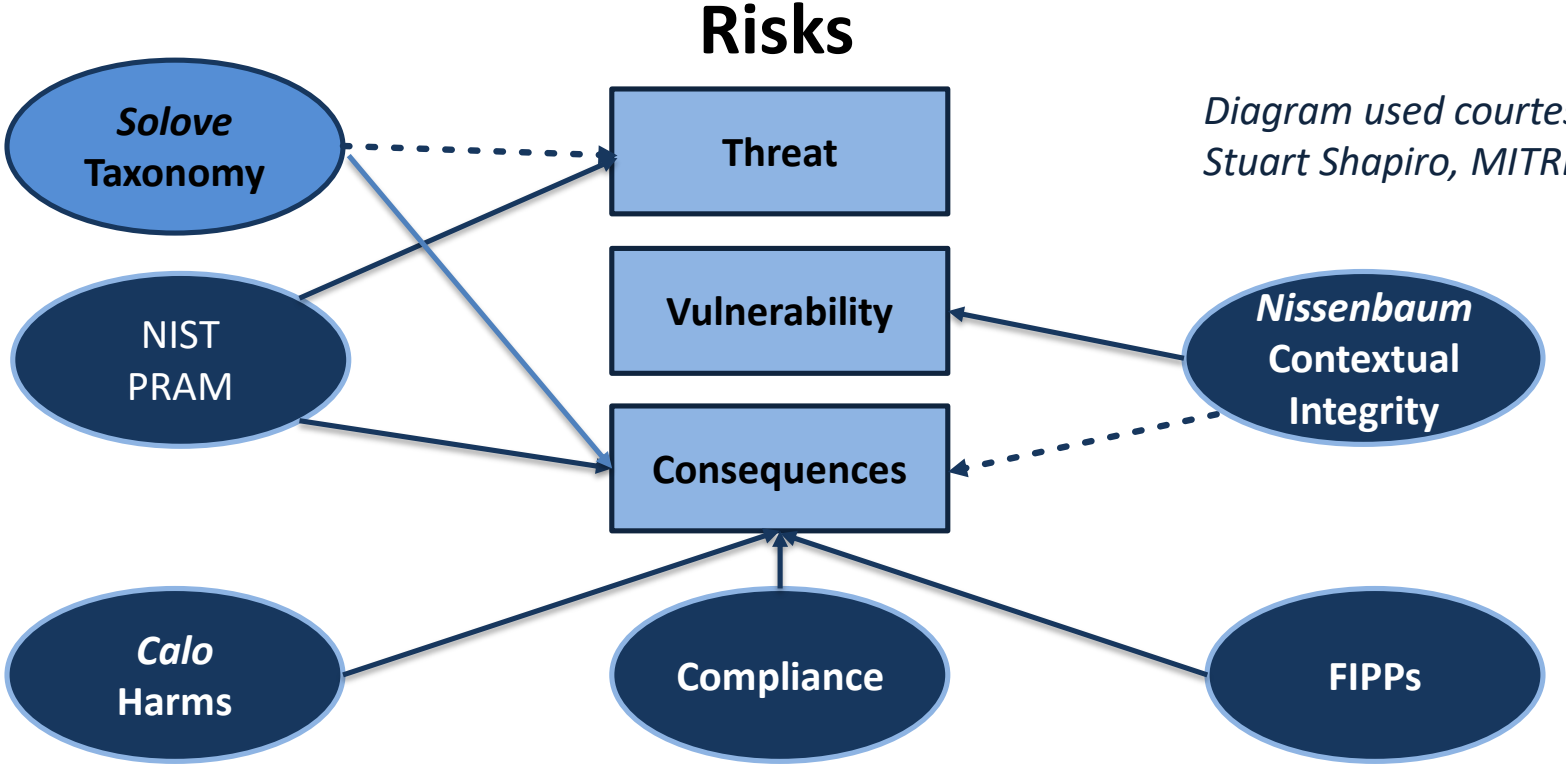


Diagram used courtesy Stuart Shapiro, MITRE

Privacy Controls

Privacy+ Security Forum

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

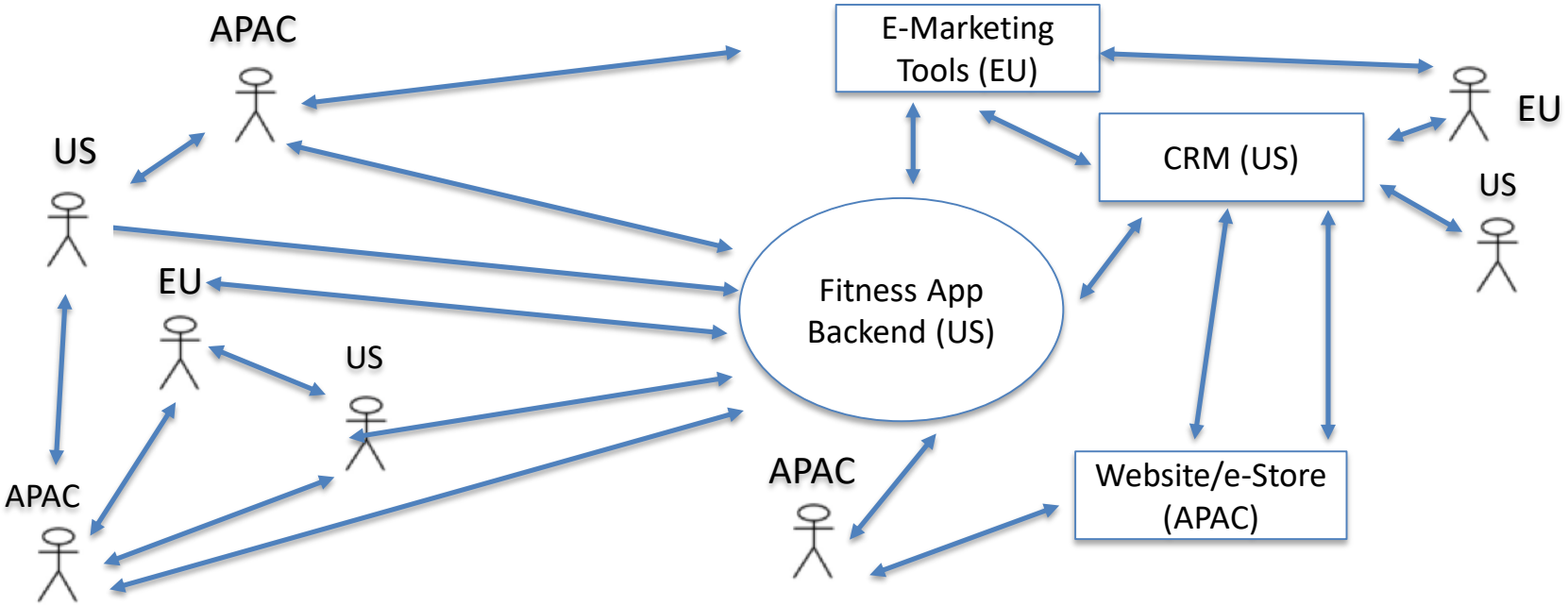
- MINIMIZE
- SEPARATE
- ABSTRACT
- HIDE
- ENFORCE
- DEMONSTRATE
- INFORM
- CONTROL

Privacy Context Diagram

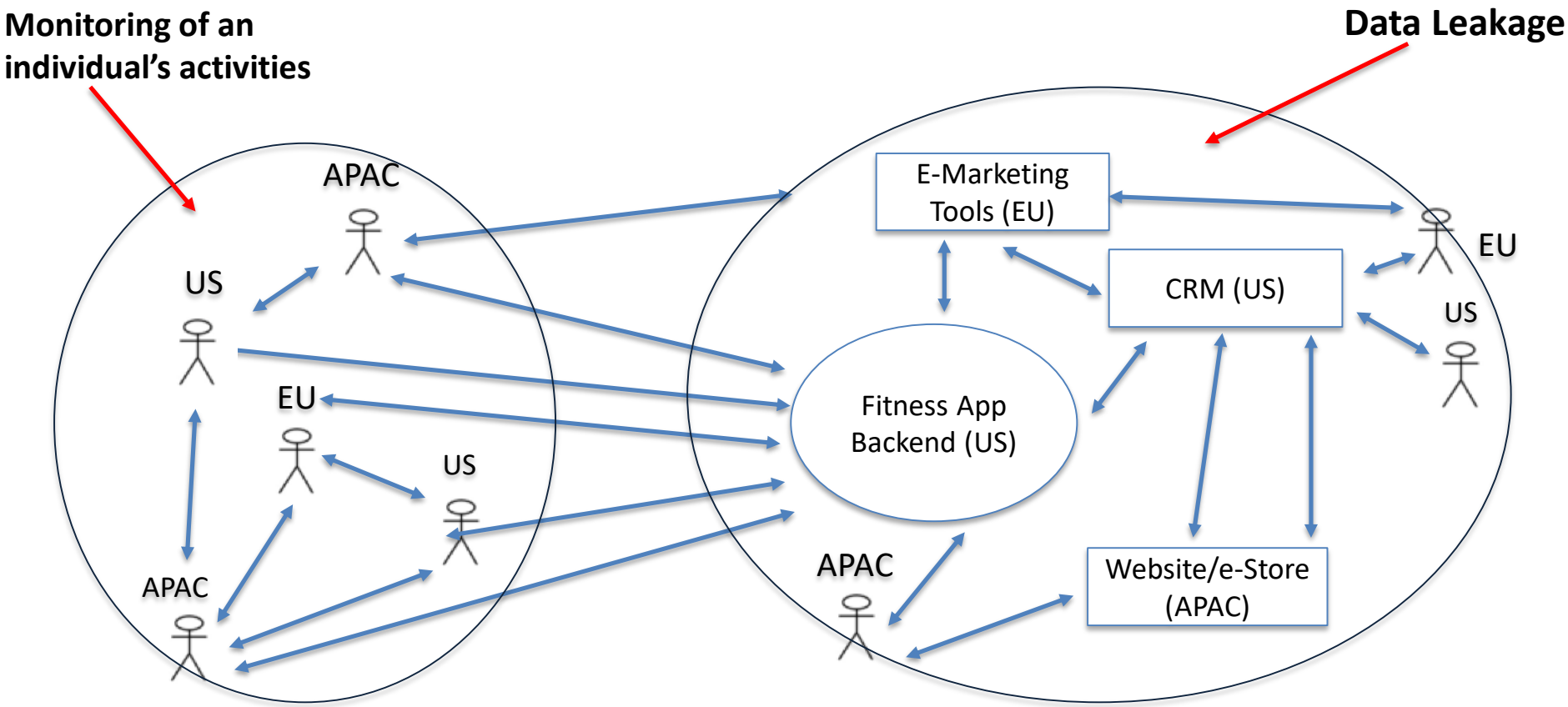
How to build a context diagram and layer in threats and controls

Privacy+ Security Forum

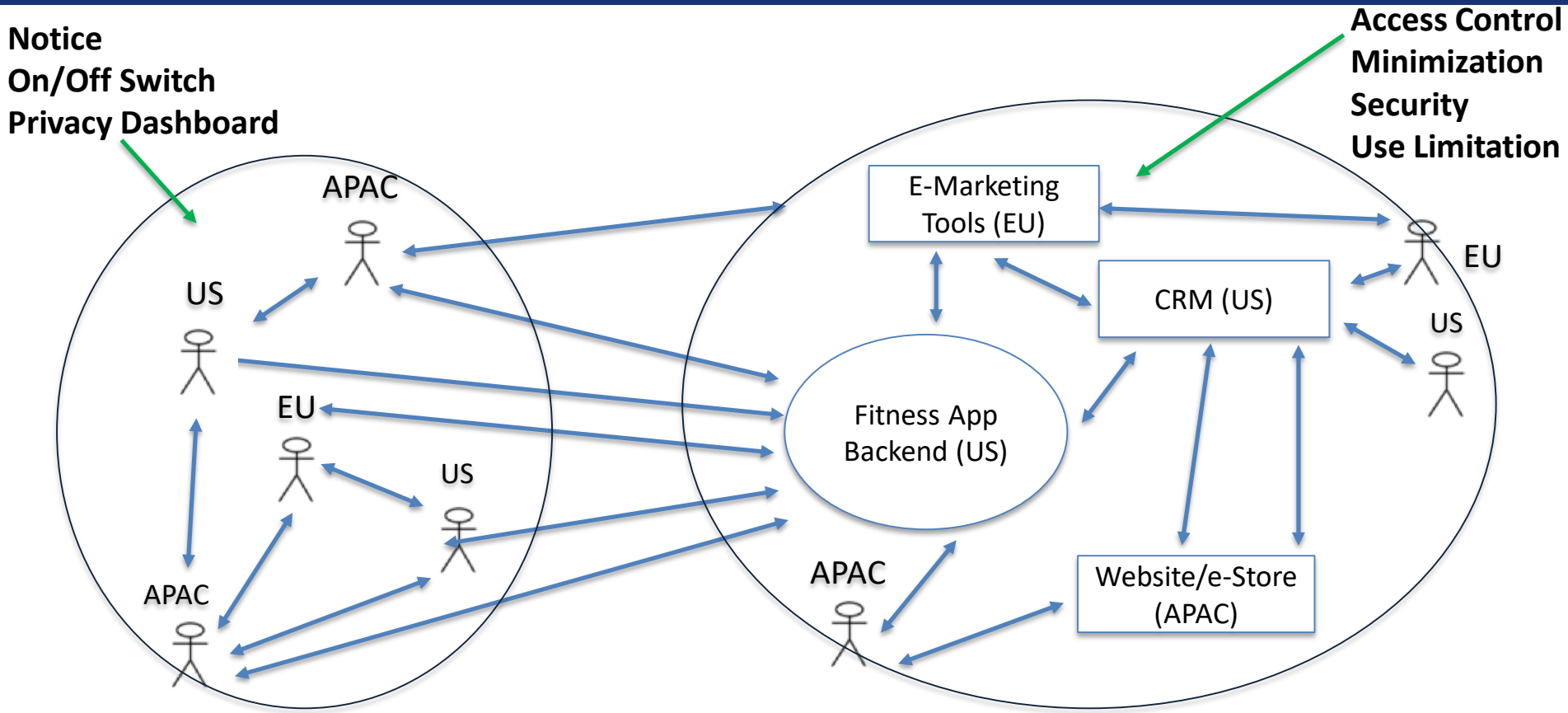
Build of a Context Diagram



Layer in Threats



Layer in Controls



Privacy Requirements & Validation

User stories make discussions more concrete and Agile definition of “Done” drives the validation of privacy requirements

User stories make discussion concrete

Privacy+ Security Forum

- **Title:** Fitness App allows user to share exercise/fitness activities
  - **As a** fitness app user
  - **I want** to share my exercise activities
  - **So that** my personal trainer can monitor my progress and keep me accountable

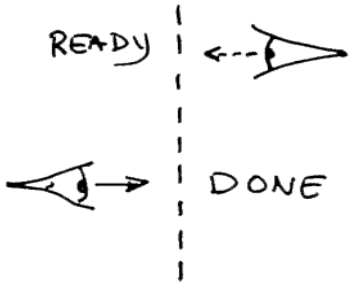
Requirement

- **Scenario:** User allows personal trainer to view exercise activities
  - **Given** exercise logs are private by default
  - **When** I change my exercise logs setting
  - **Then** my personal trainer can view my exercise logs and add comments

Acceptance Criteria

Privacy Validation

- Privacy definition of “*Done*”
- Trust but Verify > Show Me
- Final privacy review. “Go Live” sign-off



Hands-on Exercise

Apply session information

Privacy+ Security Forum

Threat Model CHARETTEE

Privacy+ Security Forum

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 two possible threats (and threat actors)
- Identify possible consequences of one of the threats
- Identify controls to mitigate the threats

Note: Business model is advertising and data monetization

Resources

Privacy+ Security Forum

Questions + Contact

Denise Schoeneich
Privacy Engineer

Intel Corporation
Denise.Schoeneich@intel.com

Jason Cronk
Privacy and Trust Consultant

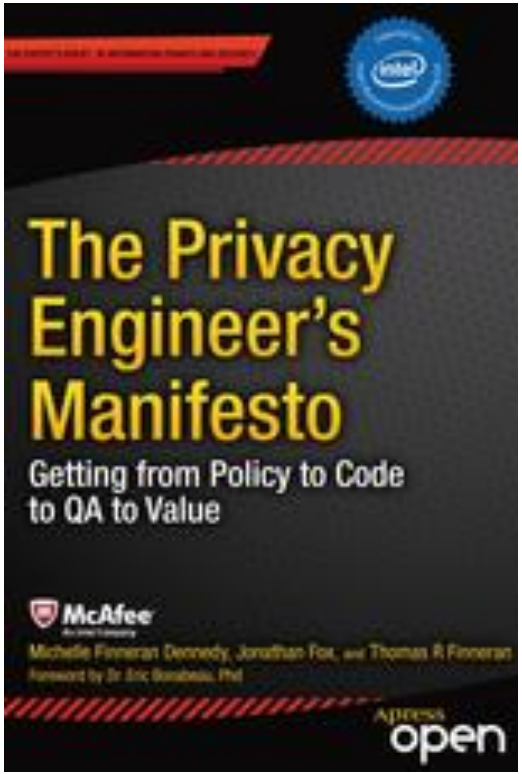
Enterprise Consulting Group
rjc@enterprivacy.com

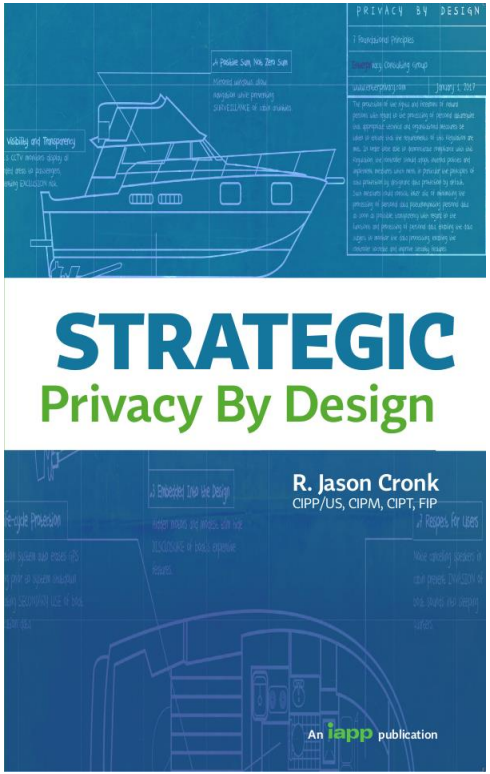
Jonathan Fox
Director, Privacy Engineering

Cisco Corporation
Jonafox@cisco.com

Shameless Self-promotion

Privacy+ Security Forum





Resources

- Annex Guide to Privacy by Design Privacy by Design Documentation for Software Engineers Version 1.0 (OASIS)
- Architecture of Privacy (O'Reilly Media)
- Clear Acceptance Criteria and Why They're Important (RubyGarage)
- Core Software Security: Security at the Source (CRC Press)
- Linddun Privacy Threat Modeling (LINDDUN)
- P7002 - Data Privacy Process (IEEE Standards Association) - 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)
- Privacy Requirements Definition and Testing (MITRE)
- Strategic Privacy by Design (IAPP)
- Taxonomy of Privacy (University of Pennsylvania Law Review)
- User stories – examples and usage (AppChance)