RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: LAB4-R08

Privacy Engineering Demystified – You too can be a Privacy Engineer

Michele D. Guel
Distinguished Engineer
Security Business Group
Cisco
@MicheleDGuel

Deepika Gupta
Security Architect/ Technical Leader
Security & Trust Organization
Cisco
@deepika00gupta

Khadija Amin
Cloud Security Architect,
Collaboration Security
Cisco
@khadijamin

Workshop Flow

- Facilitator intro
- Table set-up & Handouts
- Ice Breaker Activity
- Privacy Engineering Foundations
- Class Exercises (5)
- Class Discussion & Wrap

RSAConference2020

Ice Breaker Activiti (5 minutes)

Introduce yourself and share one of your favorite and trusted mobile apps you use on a regular basis.

Provide one example of personal information you have provided to this app. Discuss why you trust the app to protect your information

Pick first person to lead (we'll rotate clock-wise as we go through exercises)

RSAConference2020

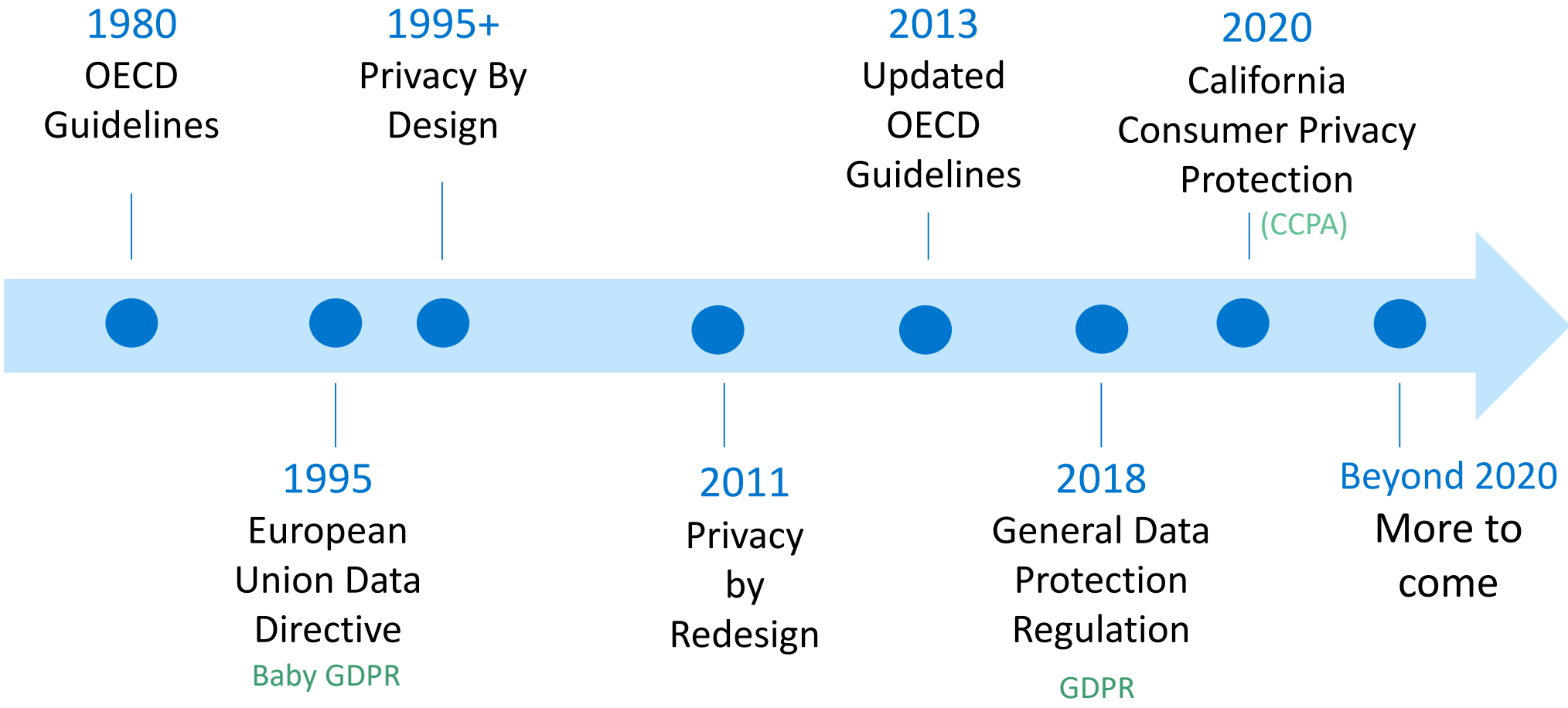
The basics of Privacy Engineering

Foundational Terminology

- GDPR
- CCPA
- Data Controller
- Data Element
- Data Owner
- Data Steward
- GAPP
- Privacy Policy
- Data Processing
- …others

See table handout for definitions

The privacy landscape has changed … and so must our design processes



The Impact of GDPR…

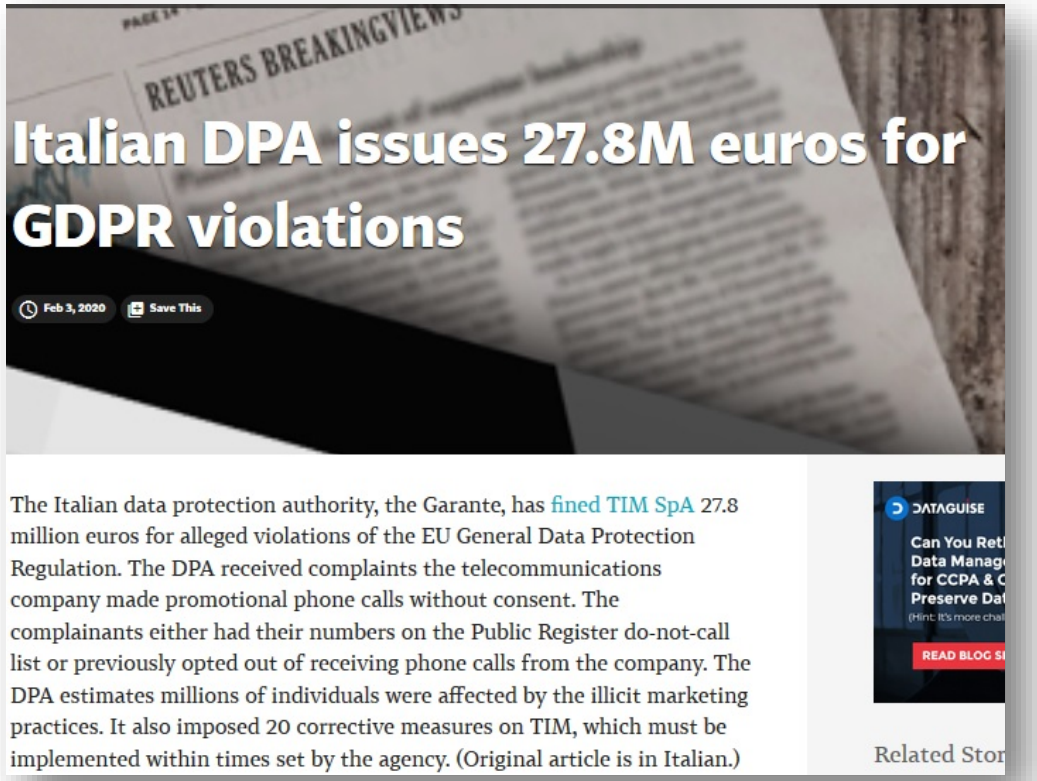
1998 EUDR

Baby Shark Bite

2018 GDPR

Megalodon Shark Chomp

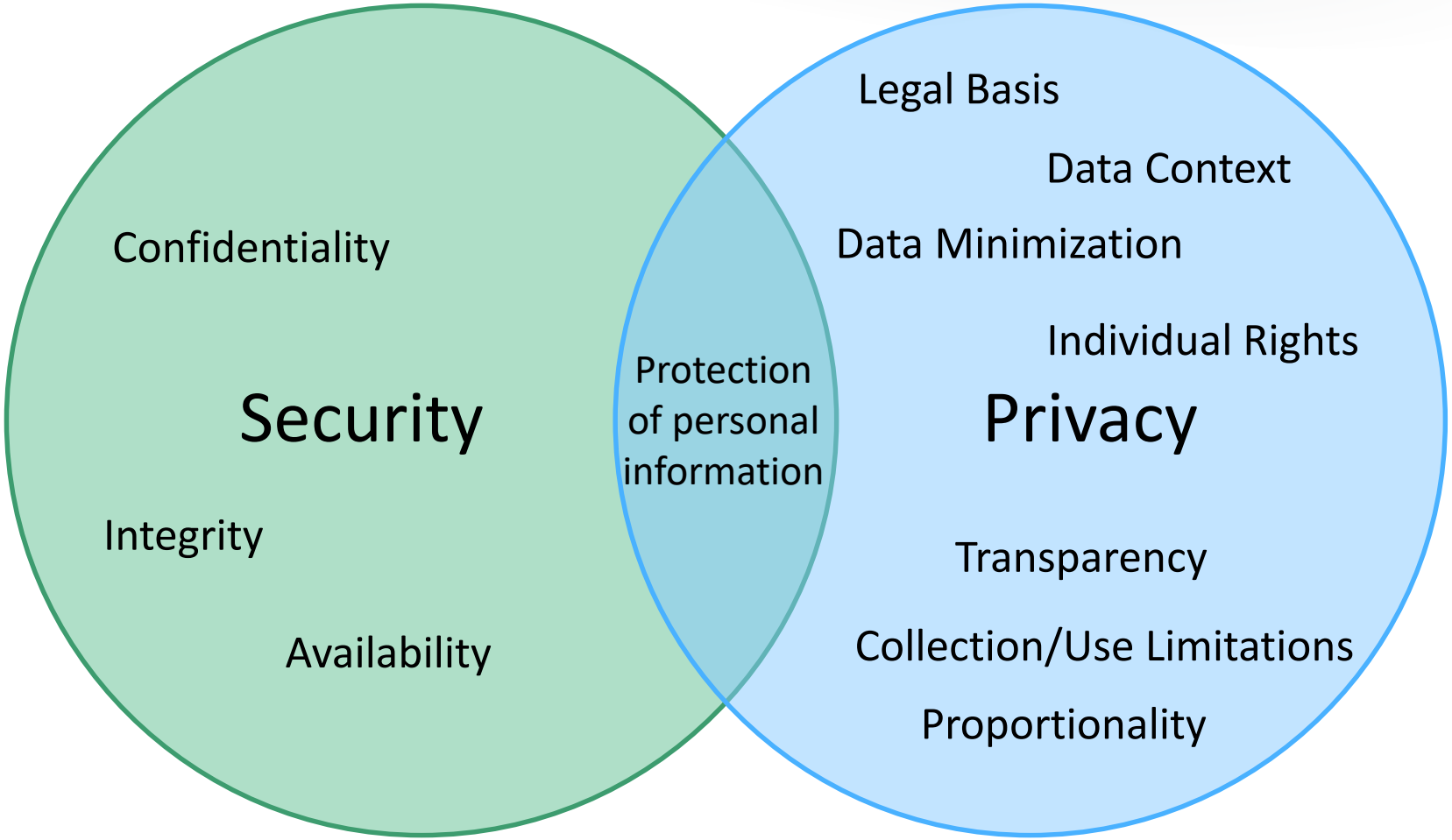
Need more motivation?



RSAConference2020

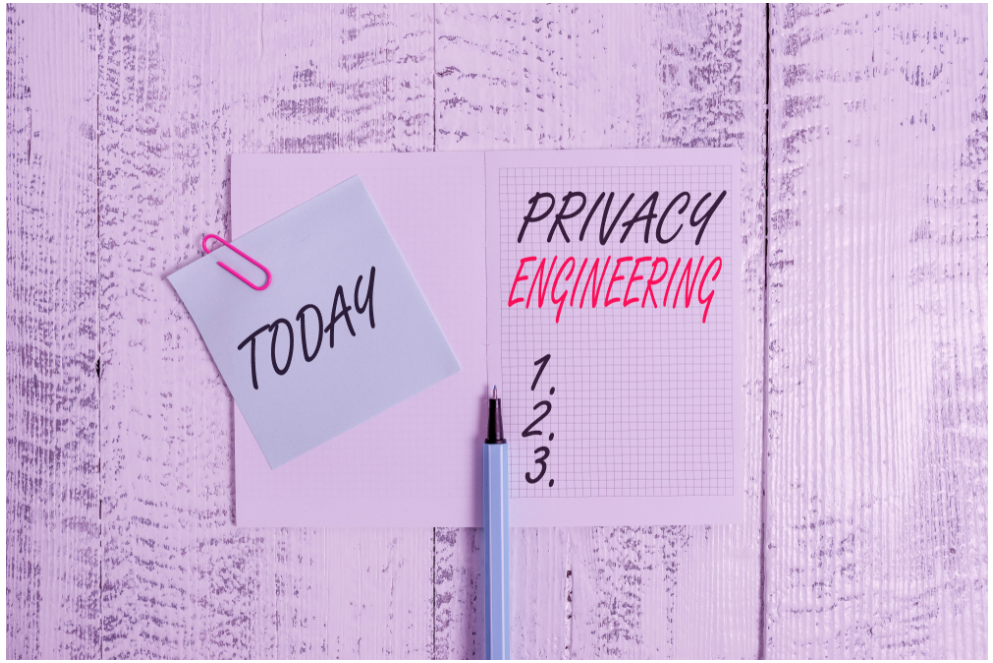
Class Discussion: Share some examples of design flaws that may lead to regulatory fines.

Security and Privacy Differences

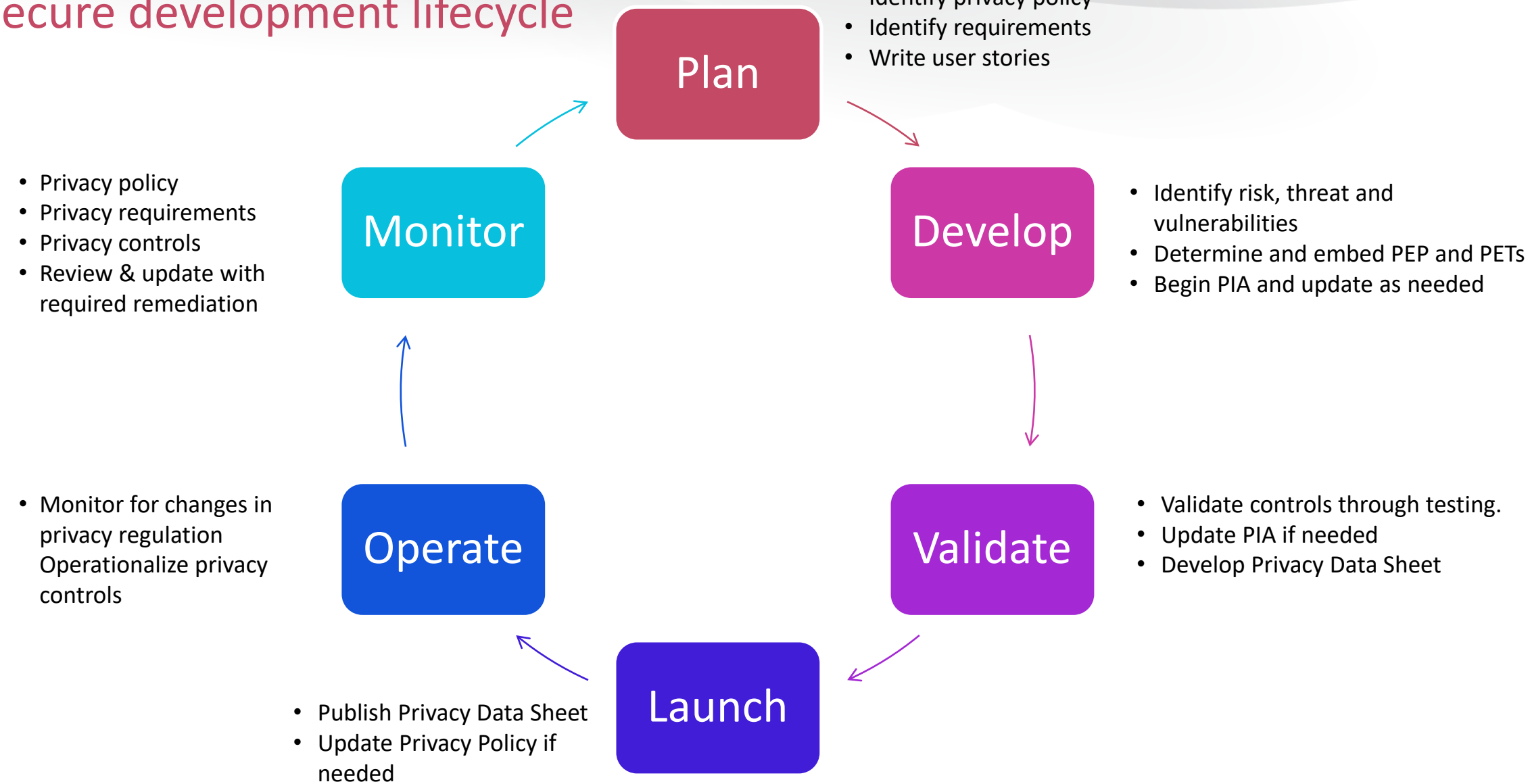


What is Privacy Engineering?

"A methodology to design, build, and manage "things" that process PII in a manner that provides appropriate levels of privacy throughout the lifecycle of the data that is processed."



Privacy Engineering as part of the secure development lifecycle



Privacy Engineering "Framework"

The technical architecture and controls should address the following areas:

- Data Context
- Legal Basis
- Accountability and Operational Requirements
- Data Minimization
- Retention and Deletion
- Individual Rights
- Security
- Transparency
- Use Limitations
- Collection Limitations
- Onward Transfer
- Proportionality

RSAConference2020

Use Case Overview and Class Exercises

Use Case Overview – HealthyAndFreshForU App

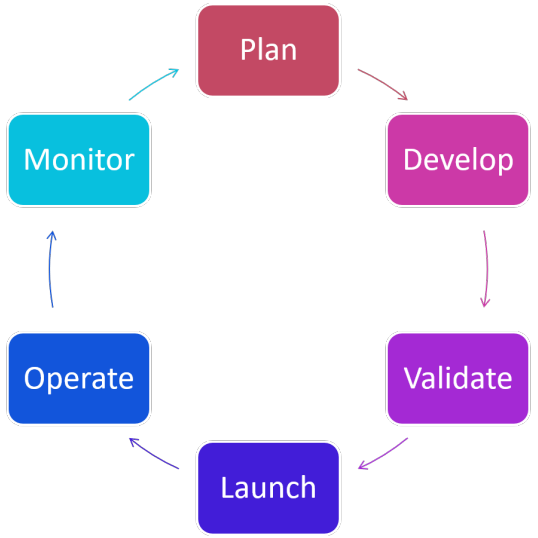
- Health food ordering mobile application.
- Subscribe to multiple health food markets and fast (but healthy) food restaurants.
- Requires registration and profile creation.
- Customize your profile based on dietary goals, favorite foods and dietary or allergy restrictions.

Basic Application Requirements

- Authenticated login (username/password).
- Profile must contain:
  - Full name, email address and mobile contact number
- Profile may contain:
  - DOB, food favorites, food allergy information, dietary restrictions, billing address, credit card information, preferred food providers, preferred delivery vendor, repeat order information
- Each order must specify:
  - Mobile phone, delivery address, credit card information, name of person to receive order.
- User must choose email or txt for receipt.

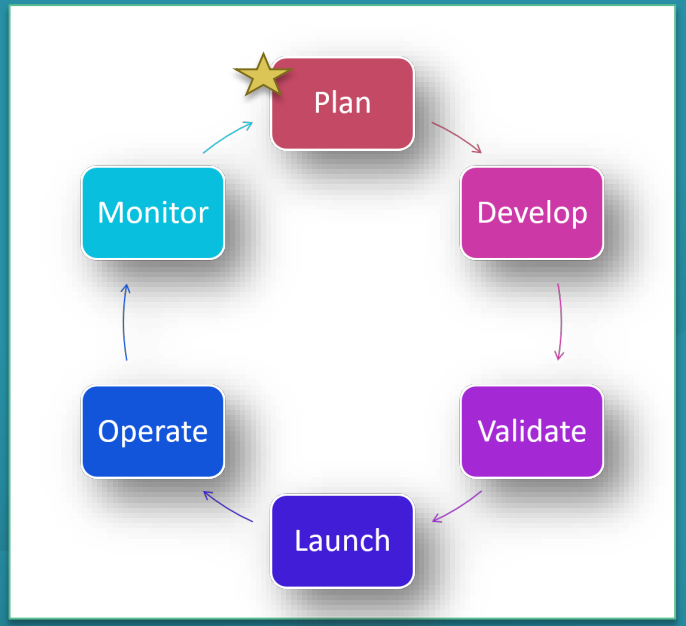
Workshop Exercises – Focus on first two phases

- Plan Phase:
  - Exercise 1: Scope the data and write the data inventory
  - Exercise 2: Review use case diagram & develop requirements
  - Exercise 3: Create user stories
- Develop Phase:
  - Exercise 4: Identify risk, threat and vulnerabilities
  - Exercise 5: Map privacy user stories to PEPs and PETs
  - Exercise 6: Begin privacy impact assessment

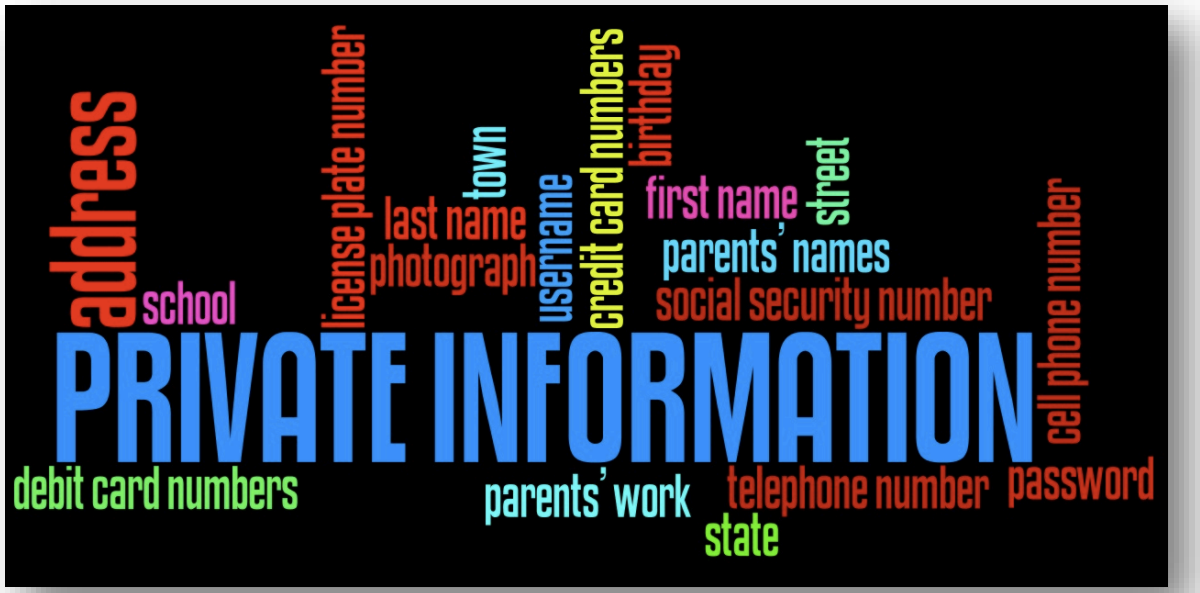


RSAConference2020

Exercise 1: Scope the data and understand the context



Is it Personal Information?



Any data that identifies an individual or from which you can derive identify or contact information of an individual. This includes otherwise non-personal information when you associate or combine with personal data.

Privacy is the fair and authorized processing of personal information or PII.

Data Context Matters!

- The context in which the data is collected and transacted must be considered and defined.
- Often an entity will collect and transact data in the context of services provided to the end user.
- For example, a corporation will collect and use employee's person data in the context of the relationship of the corporate with the employee.

Categories of PII

- Direct PII (Linked Information)
  - any piece of personal information that can be used to identify an individual
  - Examples : Full Name, Date of Birth, Email Address
- Indirect PII (Linkable Information)
  - information that on its own may not be able to identify a person, but when combined with another piece of information could identify, trace, or locate a person.
  - Examples : Gender, Race, Full name
- Sensitive PII
  - is defined as information that if lost, compromised, or disclosed could result in substantial financial loss
  - Example : Social Security Number, Credit card number, Bank account Number

Data Inventory

- Performing a data inventory would be one of the first steps in a privacy workshop. We have completed it here for you today to expedite the workshop.
- You must consider if the app is “collecting”, “storing” or “processing” information.

First Name	Preferred Food Providers	Profile login name
Last Name	Preferred Delivery Vendors	Profile Password
Email Address	Delivery Address	Daily Calorie Goal
Mobile Contact Number	Name of person receiving order	
Date of Birth	Repeat order information	
Favorite Foods	Billing Address	
Food Allergies	Credit Card Information	
Dietary restrictions	Drivers License Number	

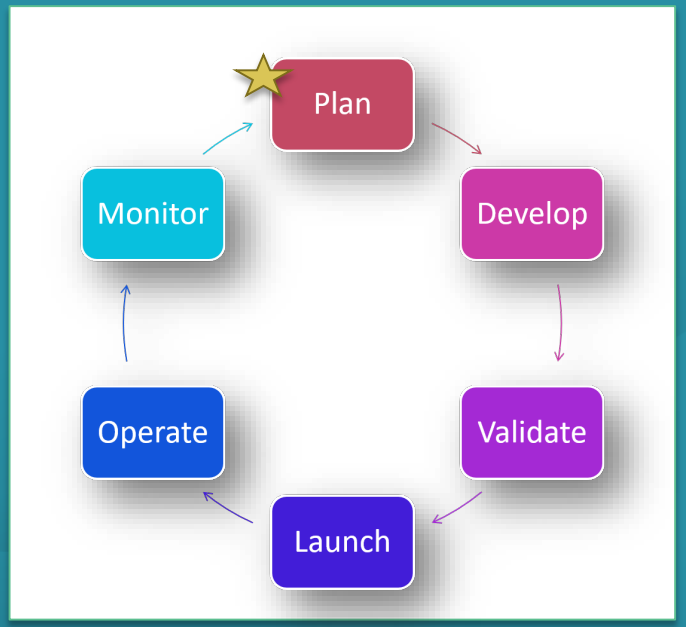
Table Exercise: Classify data element by type of PII (5 min)

- In this exercise, use the data inventory in previous slide and the data element to the column it pertains.
- Use Worksheet 1 to complete this exercise.
- Let's do a few examples: Favorite foods, delivery address, Billing address

Not PII	Direct PII	Indirect PII	Sensitive PII

RSAConference2020

Exercise 2: Review use case diagram and identify privacy requirements



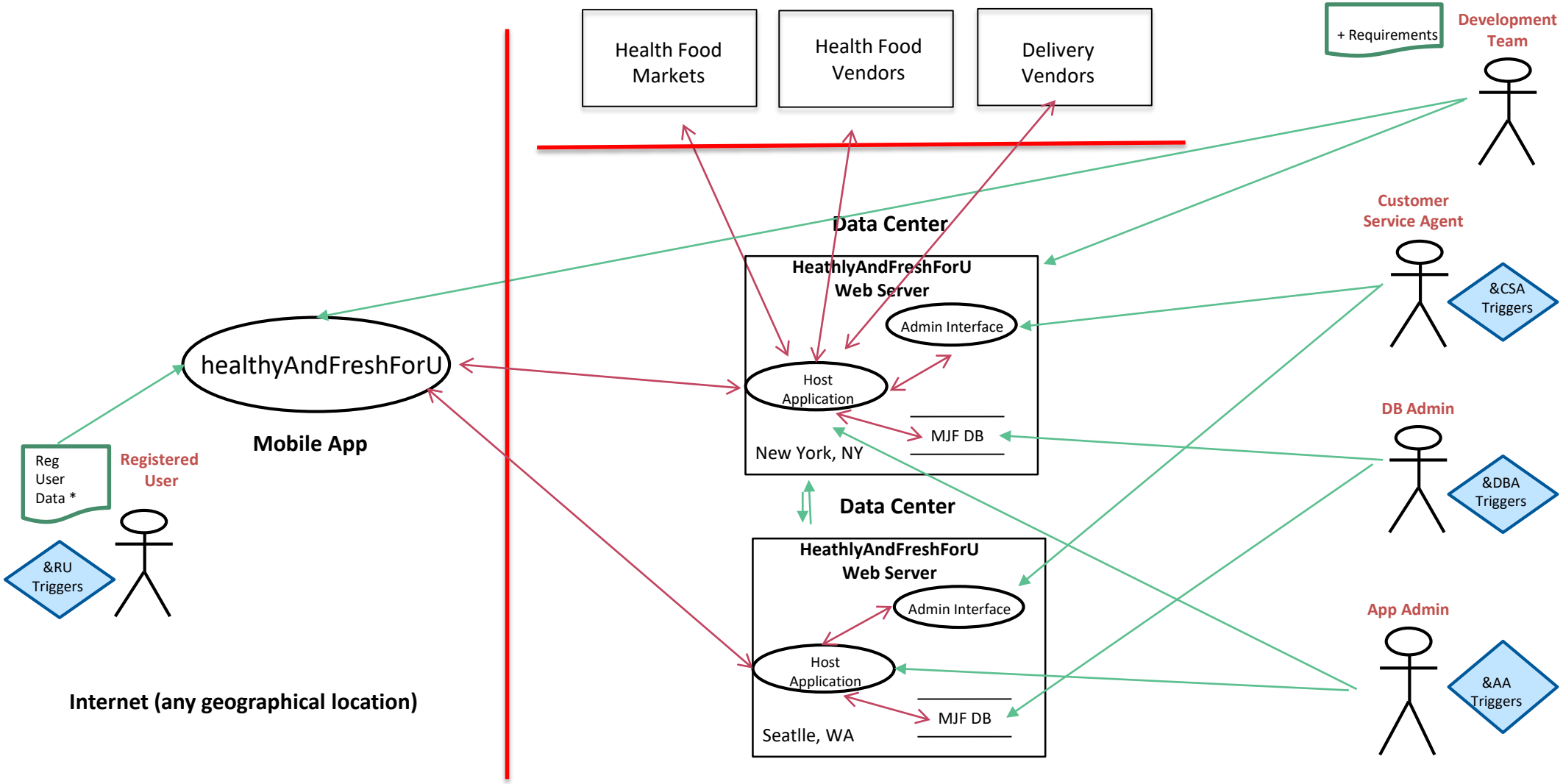
Privacy Requirements Evolve from the Privacy Policy

A **privacy policy** is a statement or a legal document (in privacy law) that discloses some or all of the ways a party gathers, uses, discloses, and manages a customer or client's data. It fulfils a legal requirement to protect a customer or client's privacy.

Typical Elements

- Collection of personal information
- Use of personal information
- Access to and accuracy of your personal information
- Your “choices” and selecting your communication preferences
- Sharing your personal information
- Security protections for your personal information
- … and more

Use Case Diagram: HealthyAndFreshForU



Identify User Personas Who Will “touch” the Data

Registered User

Customer Support

Privacy Officer

Other Potential Personas:

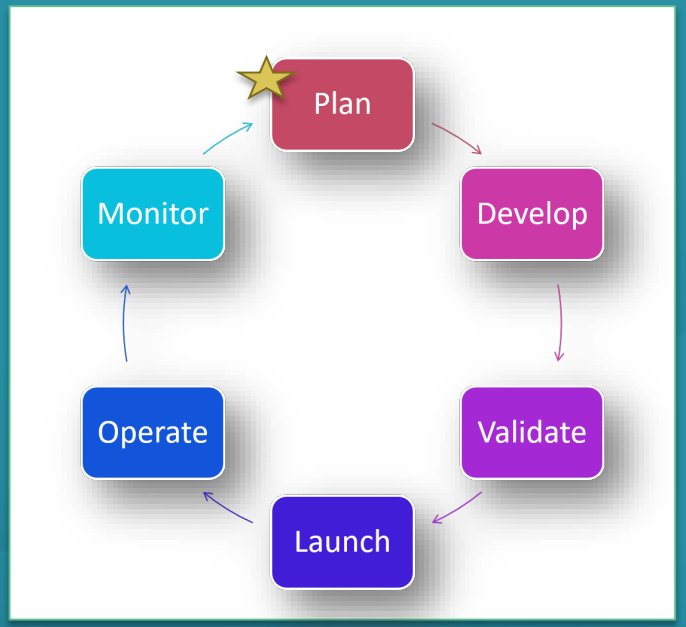
- DB Admin
- Application Admin
- Development Team Member
- Business Owner
- Delivery Person
- Credit Card Processor

Table Exercise: Review Use Case Diagram

- Using the “Discussion Guide” handout, review and answer the questions for each of the focus framework areas.
- Let’s walk through Data Context and Notice together.
- For this exercise, focus on these areas: Purpose, Collection, Minimization, and Third-party Processors.
- Discuss answers at your table.

RSAConference2020

Exercise 3: Develop user stories



Privacy User Story

- For the privacy engineer a Privacy User Story is one that is targeted at negating privacy harms or implementing privacy controls.
- Example:
  - *"As a Registered User, I need the ability to edit my profile information to correct any errors. "*
  - *"As a Developer, I need to know the single source of truth where the data will be stored so I can code the logic.*

Table Exercise: Write Privacy User Stories

- Pick two user personas from the list below:

  Register User Developer Customer Support Agent

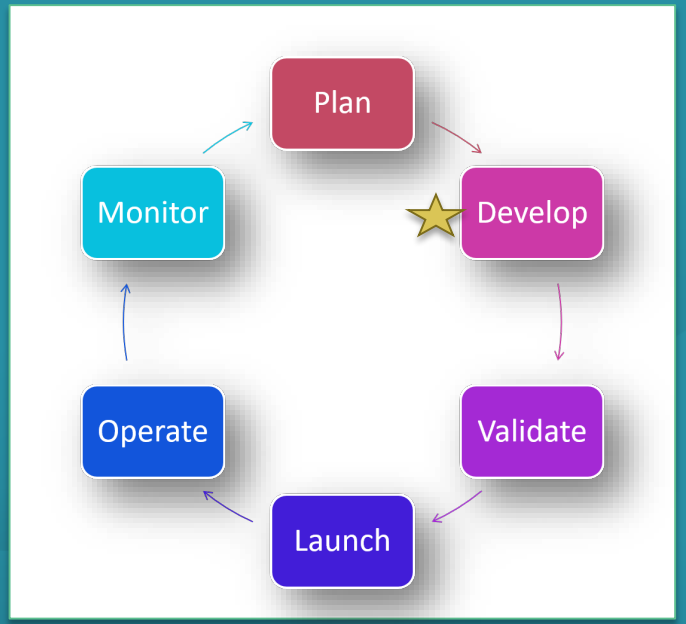
  Privacy Officer Delivery Person

- For each user persona, write 2-3 short user stories.
- Share a user story with your table.
- Use Worksheet 3 to complete this exercise.
- Let's walk through one example together.

Persona	Privacy User Story	Control Area	PET/PEP
Registered User	*"As a Registered User, I need the ability to edit my profile information to correct any errors. "*	Don't Fill in for this exercise.	Don't Fill in for this exercise.

RSAConference2020

Exercise 4: Identify risks, threats and vulnerabilities



The importance of understanding privacy risk and threats

- The privacy control frameworks are designed to help prevent threats, vulnerabilities and risks from happening.
- Gaps in controls or incorrect implementation of controls introduces risk and creates vulnerabilities that threats can take advantage of and cause harm.
- In class exercise 6, we will consider if the risks are addressed by design/controls.

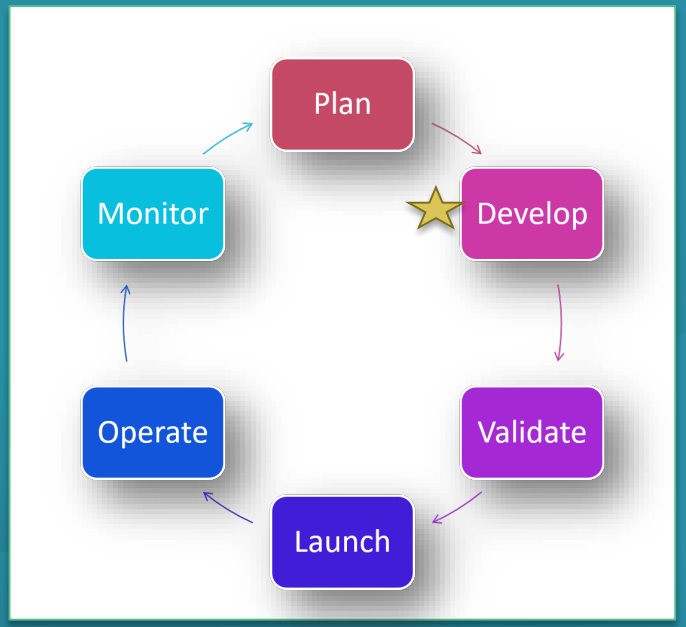
Term	Definition	Example
Asset	The object of focus for the threat actor (either directly or indirectly) to use as a stepping stone to get to desired object.	User medical records.
Threat	Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage or destroy an asset.	An internal bad actor looking to steal PII.
Vulnerability	A weakness or gap in our protection and data management efforts that can be exploited by threats to gain unauthorized access to an asset.	No visibility to anomalous user behavior (e.g. No user or entity behavior analytics).
Risk	The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability. The common equation use is “Asset + Threat + Vulnerability = Risk”	A data breach involving exfiltration of 20,000 medical records from a hospital database.

Table Exercise: Identify Privacy Risks, Threats and Vulnerabilities

- For each of your user stories, think about the data captured, who the threat actor(s) might be, avenues to gain access and elements of risk for our use case.
- In this exercise, use the worksheet 4.
- Let's do one example together:
  - Asset of interest: Credit card information
  - Threat Actor: hacker interested in selling CC information
  - Vulnerability: on certain platforms, the username and password are stored in the log during authentication. Log information can be viewed by threat actors.
  - Risk: CC information can be gathered and sold.

RSAConference2020

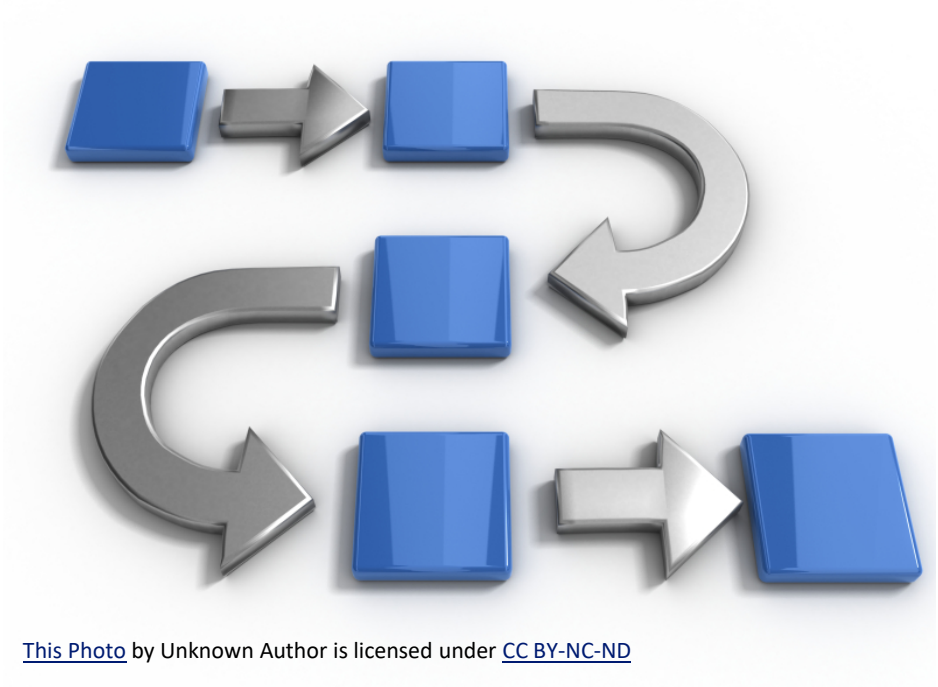
Exercise 5: Map privacy user stories to PEPs and PETs



Privacy Enhancing Technologies (PETs)

- Privacy-enhancing technologies (PETs) are the standardized term for technologies that can provide the controls necessary in the privacy policy.
- PETs provide systemic, technical controls to help protect personal information in products, offerings, solutions, and applications.
- Example technologies
  - Single sign-on identity with strong password Management
  - Hypertext Transfer Protocol Secure (HTTPS) for data transfer
  - Database row encryption

Privacy Enhancing Processes (PEPs)



- PEPs are controls implemented through process (and not technology).
- PEPs require privacy awareness and documented steps in our processes to support the privacy control categories.
- PEPs support PETs
- Example processes:
  - Web/Mobile app based purpose changes (e.g. Notice).
  - Corporate privacy policy
  - Privacy product requirements

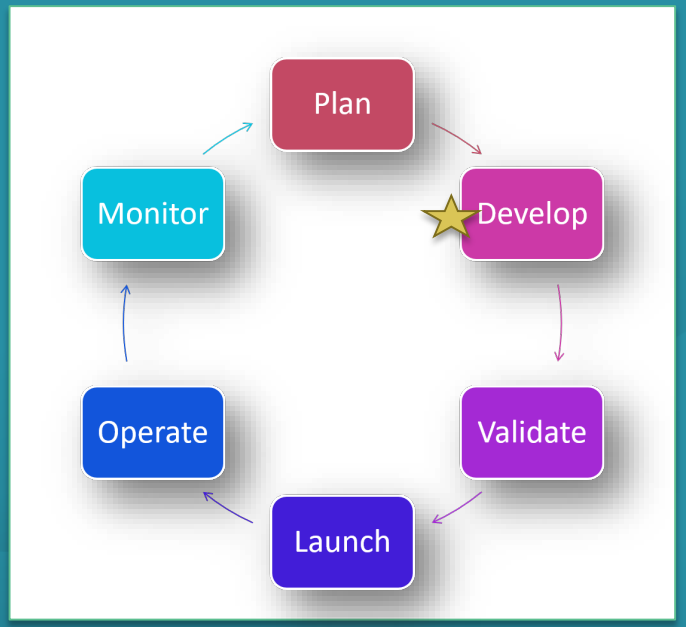
Table Exercise: Map user stories to PEPs and PETS

- In this exercise, use the privacy user stories you developed in Exercise 3.
- Consider the threats, vulnerabilities and risk you outlined in Exercise 4.
- Identify the control area and a PET/PET to address the risk.
- User worksheet 3 again, focus on last two columns.
- Let's do one example together:

Persona	Privacy User Story	Control Area	PET/PEP
Developer	"As a developer, I need to make sure end to end operation of user's data is minimized. For example full credit card is not displayed on view profile. "	Data Minimization	Data Masking

RSAConference2020

Class Exercise 6: Privacy Impact Assessment



The Privacy Impact Assessment (PIA)

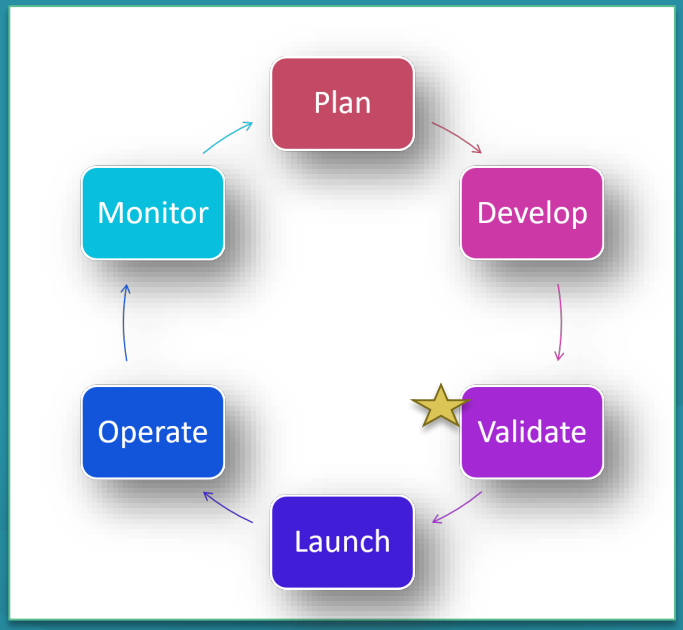
- The PIA is a process for managing risks to data privacy caused by the processing of personal data.
- The PIA provides a systematic means of answering questions like:
  - How is the data it being collected, processed and stored?
  - What are the existing controls for data protection?
  - What aspects of processing can potentially cause harm to concerned individuals, the organization, or the public?
- Article 35 of GDPR *"the obligation of the controller to conduct an impact assessment and to document it before starting the intended data processing."*
- There is no one specification for a PIA.
- All the information you have documented thus far will help complete the PIA.
- Completing the PIA helps identify additional gaps.

Class Exercise: Privacy Impact Assessment

- For this exercise, see Worksheet 5 – A PIA template.
- We need to consider all the information from the previous exercises.
- Let's focus on the following sections for the exercise:
  - Data inventory
  - Collection
  - Sharing

RSAConference2020

Additional Class Discussion



Apply what you have learned today

Immediate

- Complete the class exercises.
- Review answers with out completed answer sheet.
- Share your experience with a co-worker.
- Review privacy processes in place at your organization.

Within 90 days

- Socialize importance of privacy engineering with your organization.
- Give an overview to others in your group based on this workshop.
- Expand your privacy knowledges at IAPP web portal.

Within 180 days

- Incorporate privacy engineering as part of the development process.
- Read The Privacy Engineer's Manifesto and Companion Guide.
- Take training to obtain a privacy certification.

Download our version of the answer sheet on google drive

RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **LAB4-R08**

Thank You!
Please fill out the class survey.

Michele D. Guel
Distinguished Engineer
Security Business Group
Cisco
@MicheleDGuel

Deepika Gupta
Security Architect/ Technical Leader
Security & Trust Organization
Cisco
@deepika00gupta

Khadija Amin
Cloud Security Architect,
Collaboration Security
Cisco
@khadijamin