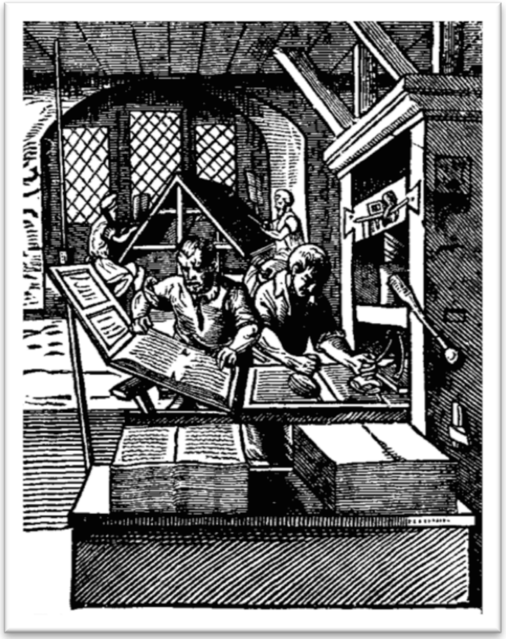
Privacy Engineering

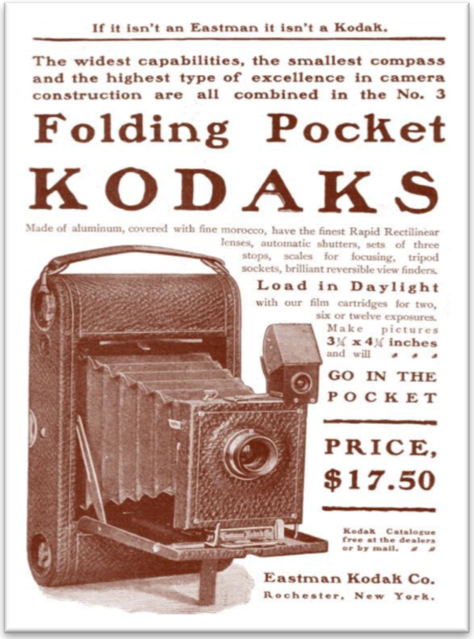
Jonathan Fox | Director of Data Privacy

Back to the Future

Technology and innovation presenting challenges to privacy is not new



Printing Press



If it isn't an Eastman it isn't a Kodak.

The widest capabilities, the smallest compass and the highest type of excellence in camera construction are all combined in the No. 3

Folding Pocket

KODAKS

Made of aluminum, covered with fine morocco, have the finest Rapid Rectilinear lenses, automatic shutters, sets of three stops, scales for focusing, tripod sockets, brilliant reversible view finders.

Load in Daylight with our film cartridges for two, six or twelve exposures.

Make pictures 3¼ x 4¼ inches and will GO IN THE POCKET

PRICE, $17.50

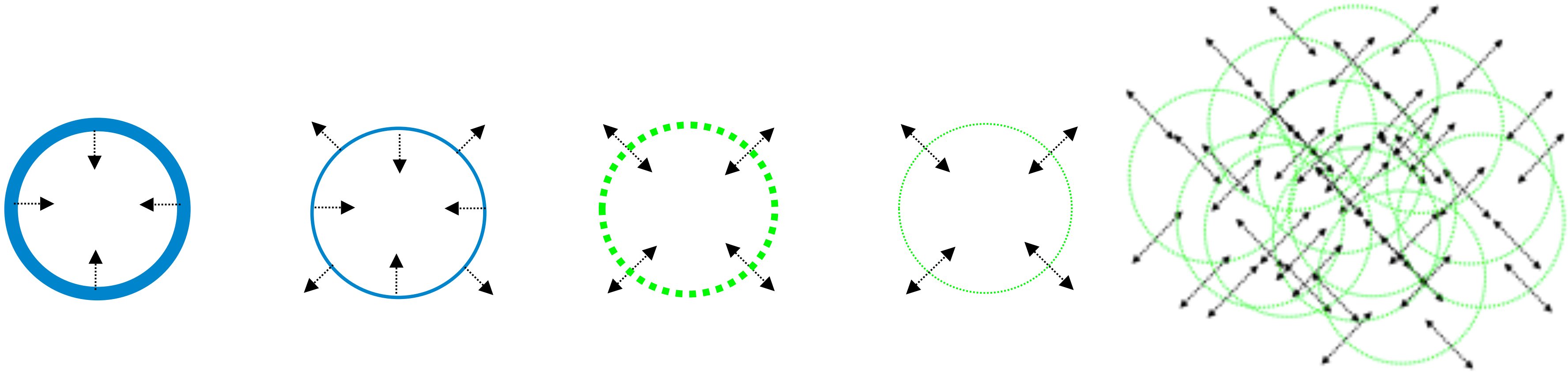
Kodak Catalogue free at the dealers or by mail.

Eastman Kodak Co.
Rochester, New York.

Camera

Database

We are in the fifth stage of the Information Age



Firewall

Keep data **within** the firewall

Net

Manage data **inside** and **outside** the firewall

Extranet

Manage data **through** the firewall

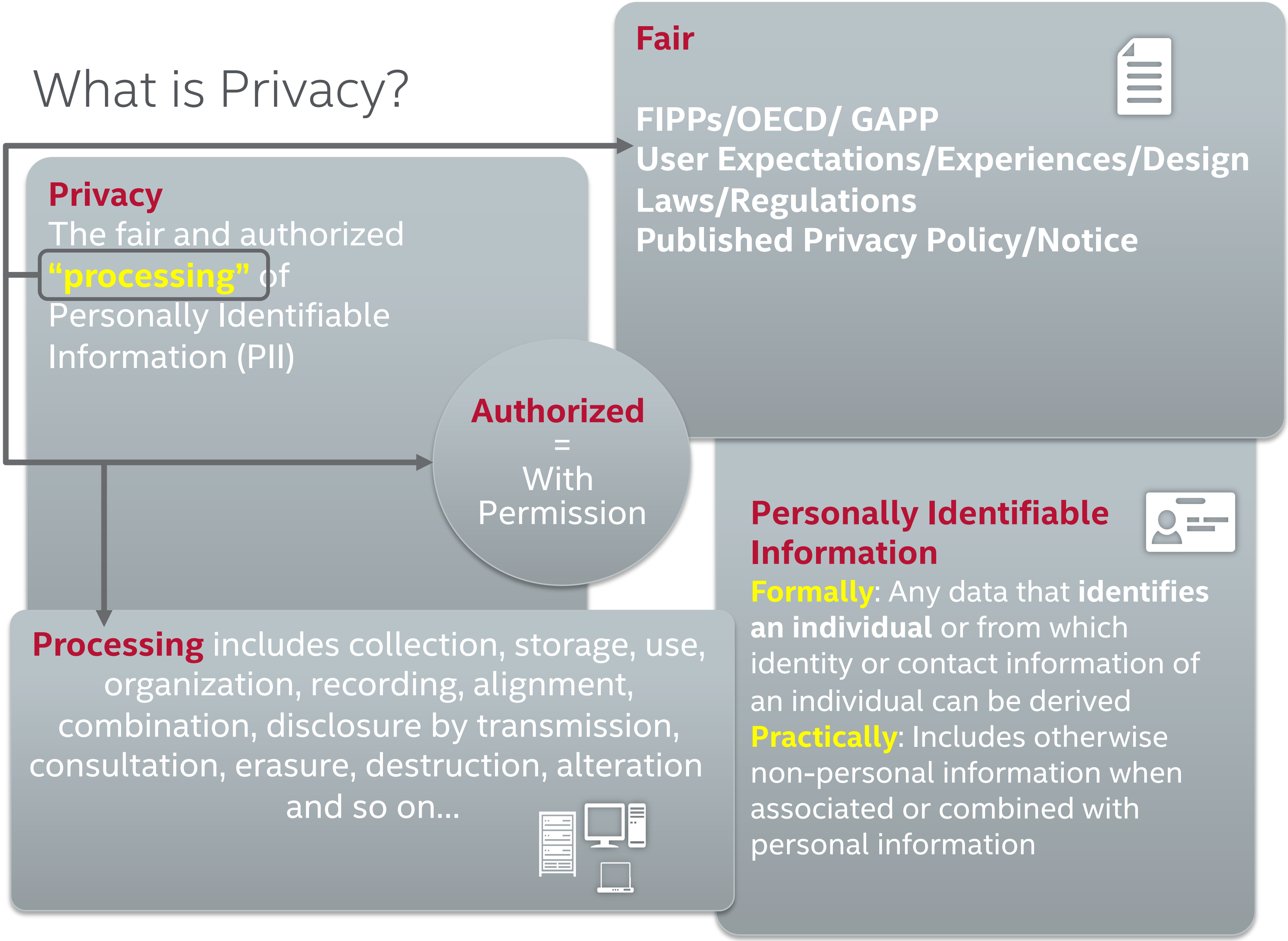
Access

Manage data through **IDM** and **access control**

Intelligence

Dynamic content **data-centric** & **person-centric**

What is Privacy?



Privacy
The fair and authorized **"processing"** of Personally Identifiable Information (PII)

Fair

FIPPs/OECD/ GAPP
User Expectations/Experiences/Design
Laws/Regulations
Published Privacy Policy/Notice

Authorized
=
With Permission

Processing includes collection, storage, use, organization, recording, alignment, combination, disclosure by transmission, consultation, erasure, destruction, alteration and so on…

Personally Identifiable Information

Formally: Any data that **identifies an individual** or from which identity or contact information of an individual can be derived

Practically: Includes otherwise non-personal information when associated or combined with personal information

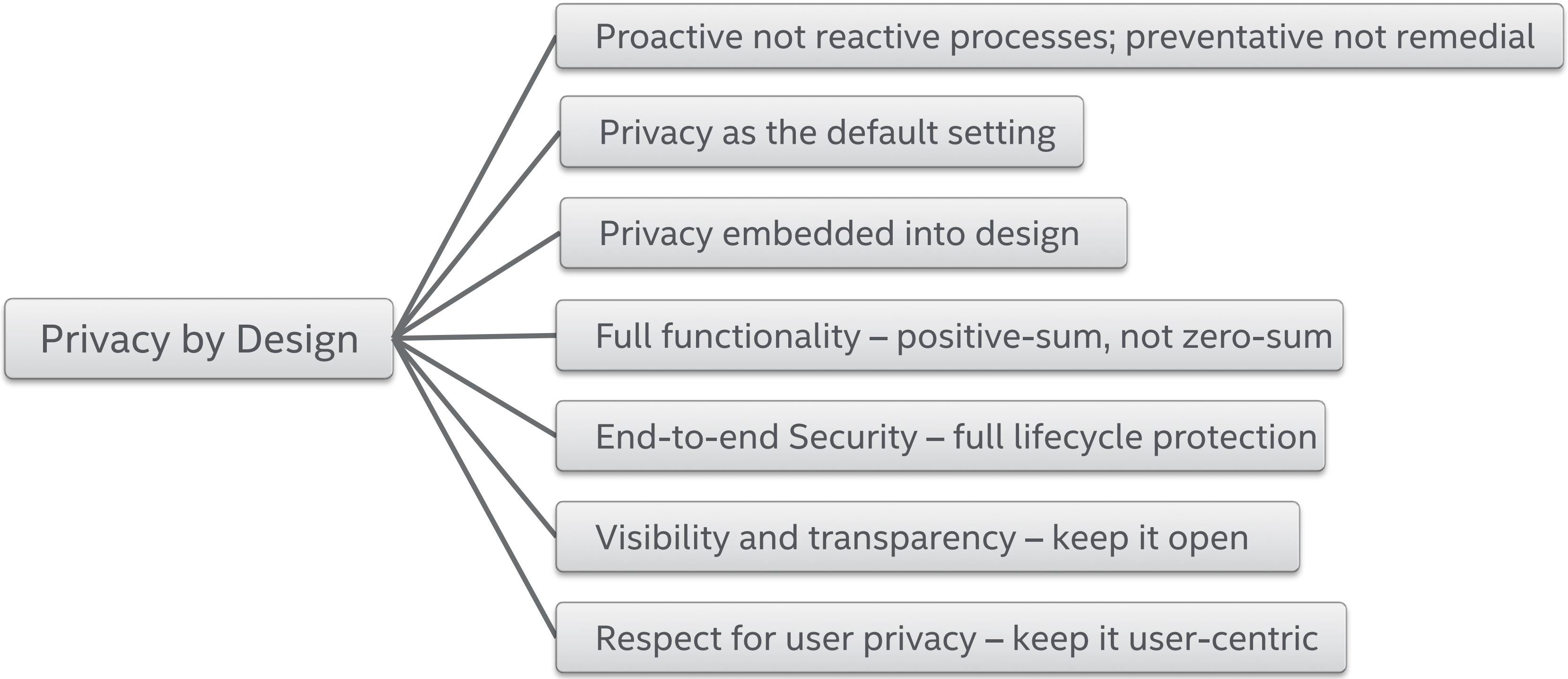
Privacy Engineering is:

A) A discrete **discipline** or field of inquiry and innovation using **engineering principles** and processes to build controls and measures into processes, systems, components, and products that enable the authorized processing of personal information.

B) The **creative innovation process** to manage increasingly more complex data streams and data sets that **describe individual humans**.

C) The gathering and application of privacy requirements with the same **primacy** as other traditional feature- or process requirements and then **incorporating, prioritizing, and addressing** them at each **stage** of the development process, project, product or system lifecycle

Privacy Engineering goes beyond Privacy by Design (PbD)



Privacy by Design

- Proactive not reactive processes; preventative not remedial
- Privacy as the default setting
- Privacy embedded into design
- Full functionality – positive-sum, not zero-sum
- End-to-end Security – full lifecycle protection
- Visibility and transparency – keep it open
- Respect for user privacy – keep it user-centric

What kind of requirement is privacy?

A) Functional

B) Nonfunctional

C) Quality Attribute

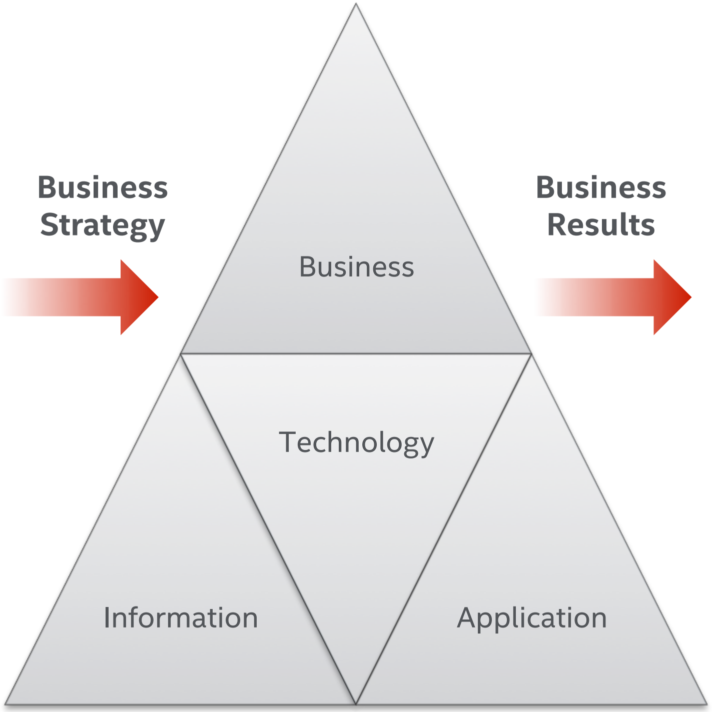
A requirement of what?

A) System Requirement

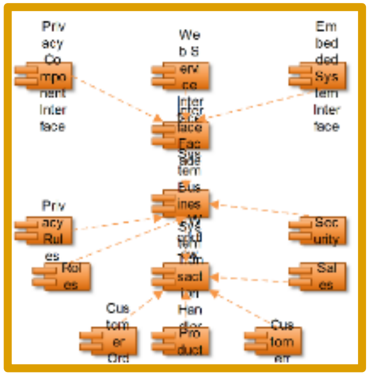
B) Data Requirement

C) Business Requirement

Its all connected

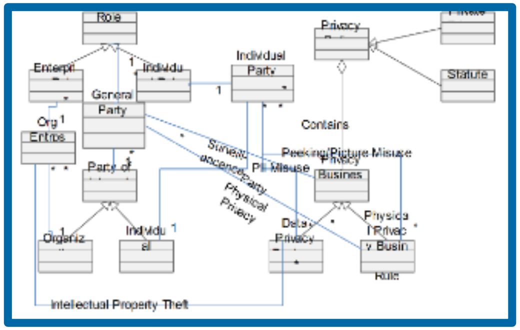


Enterprise Architecture



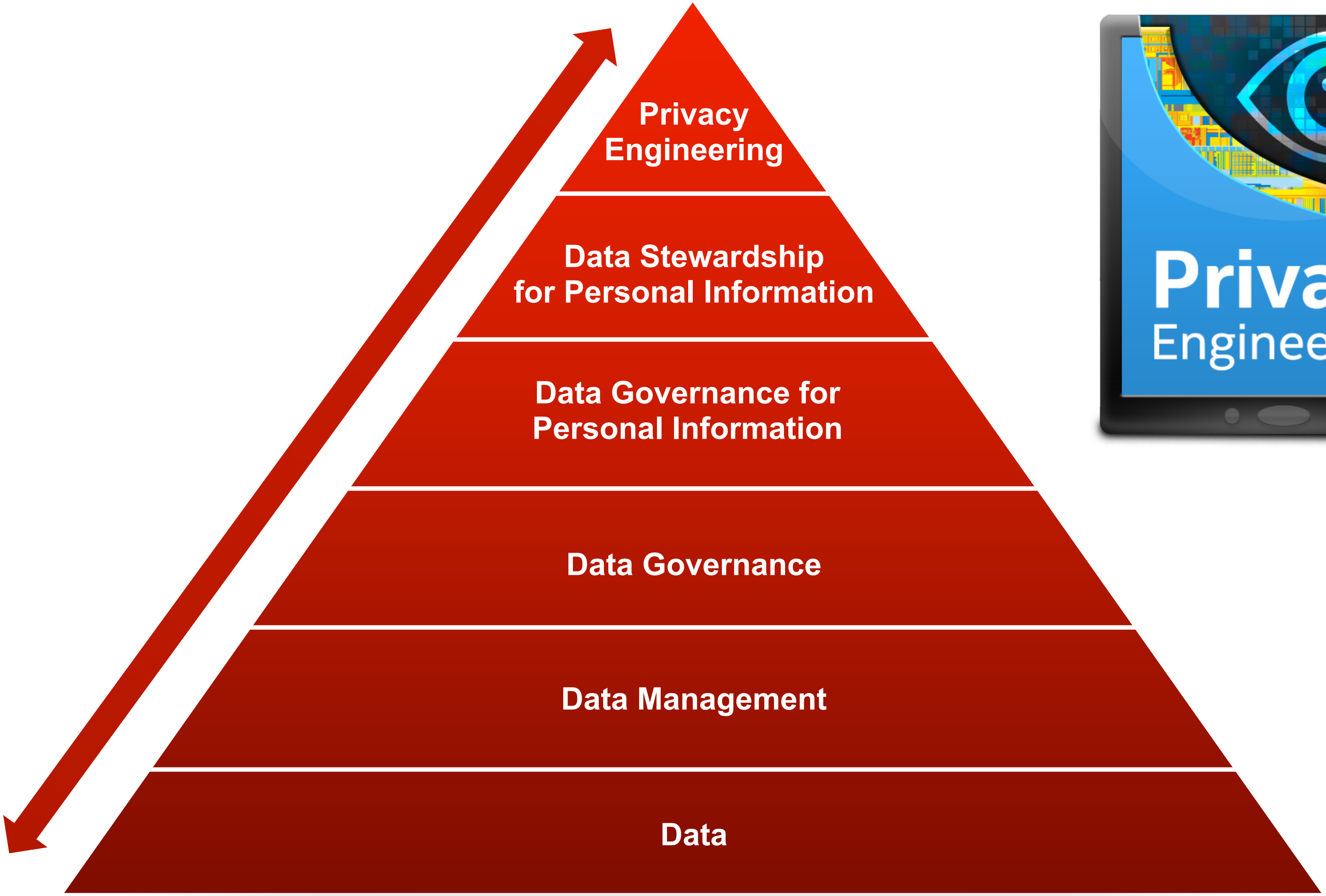
Application Architecture

User Interface Architecture

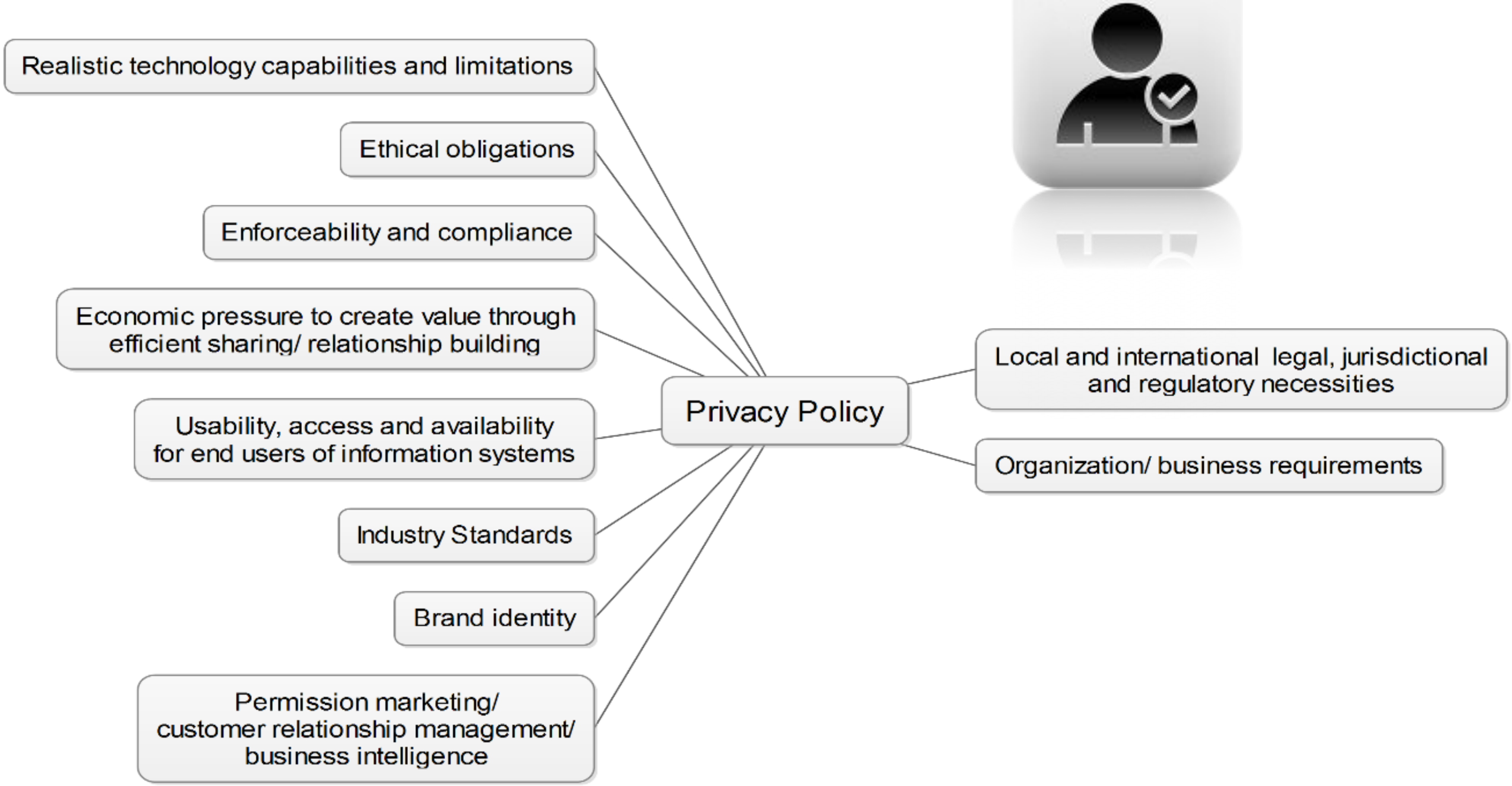


Information Architecture

Privacy is built on a foundation of data management and governance


Privacy Engineering
Data Stewardship for Personal Information
Data Governance for Personal Information
Data Governance
Data Management
Data

Think of privacy notices as meta-use case requirements



Realistic technology capabilities and limitations

Ethical obligations

Enforceability and compliance

Economic pressure to create value through efficient sharing/ relationship building

Usability, access and availability for end users of information systems

Industry Standards

Brand identity

Permission marketing/ customer relationship management/ business intelligence

Privacy Policy

Local and international legal, jurisdictional and regulatory necessities

Organization/ business requirements

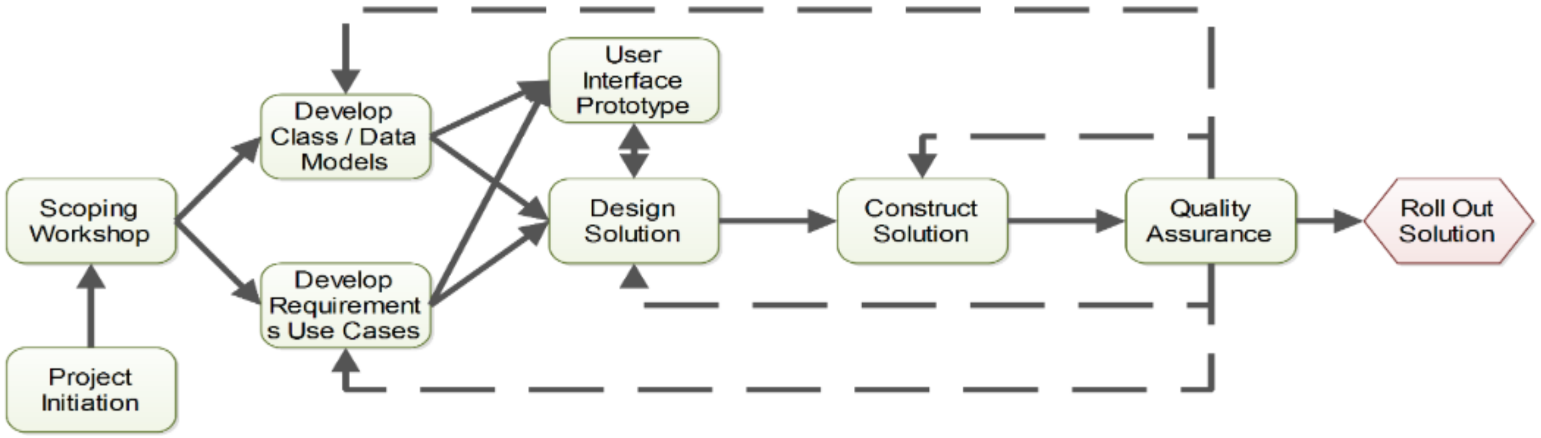
Use cases, Data Models, User Requirements

Make Privacy part of the process

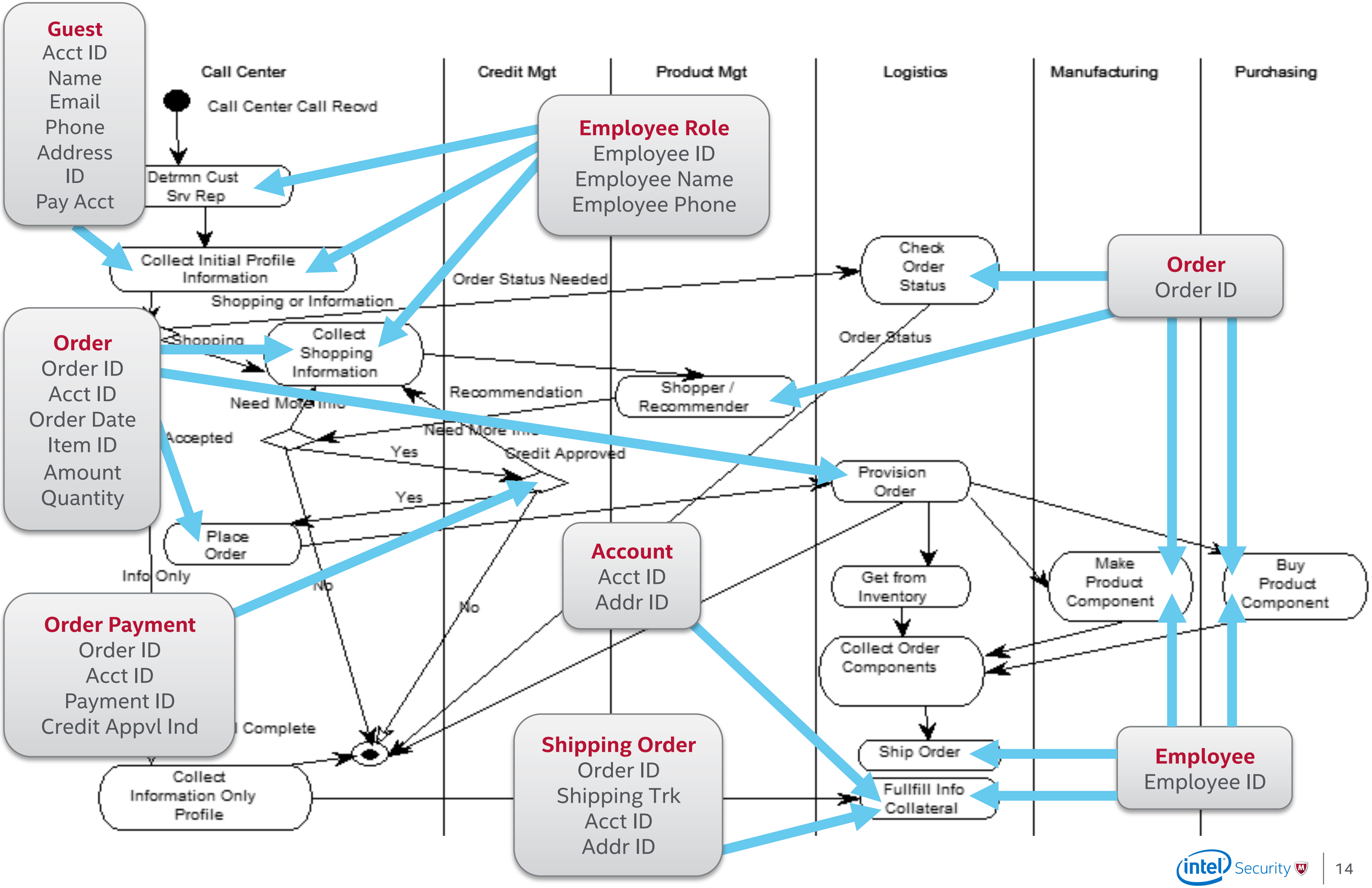
- **Use Cases -** A complete course of events initiated by a Primary Actor. These can be used to test and experiment with purpose and potential combinations of PI or can be used as a road map for Audit.
- **Business Data Model** – The model describes what data is required to perform requested functions and services.
- **User Experience Requirements** – Description of impact upon and interaction of Users who act, donate or curate upon Personal Information.

Development Life Cycle Stages

- The development of **Requirement Use Cases** and **Class/Data Models** defines the enterprise and seeks to understand the business requirements sought to be addressed.
- The **solution design** including prototyping the user interface for the project
- The **implementation** stage that includes solution construction.
- The **Quality Assurance** stage includes testing and user acceptance.
- The solution **rollout**.



Business Activity Diagrams as privacy tool



Guest
Acct ID
Name
Email
Phone
Address ID
Pay Acct

Employee Role
Employee ID
Employee Name
Employee Phone

Order
Order ID

Order
Order ID
Acct ID
Order Date
Item ID
Amount
Quantity

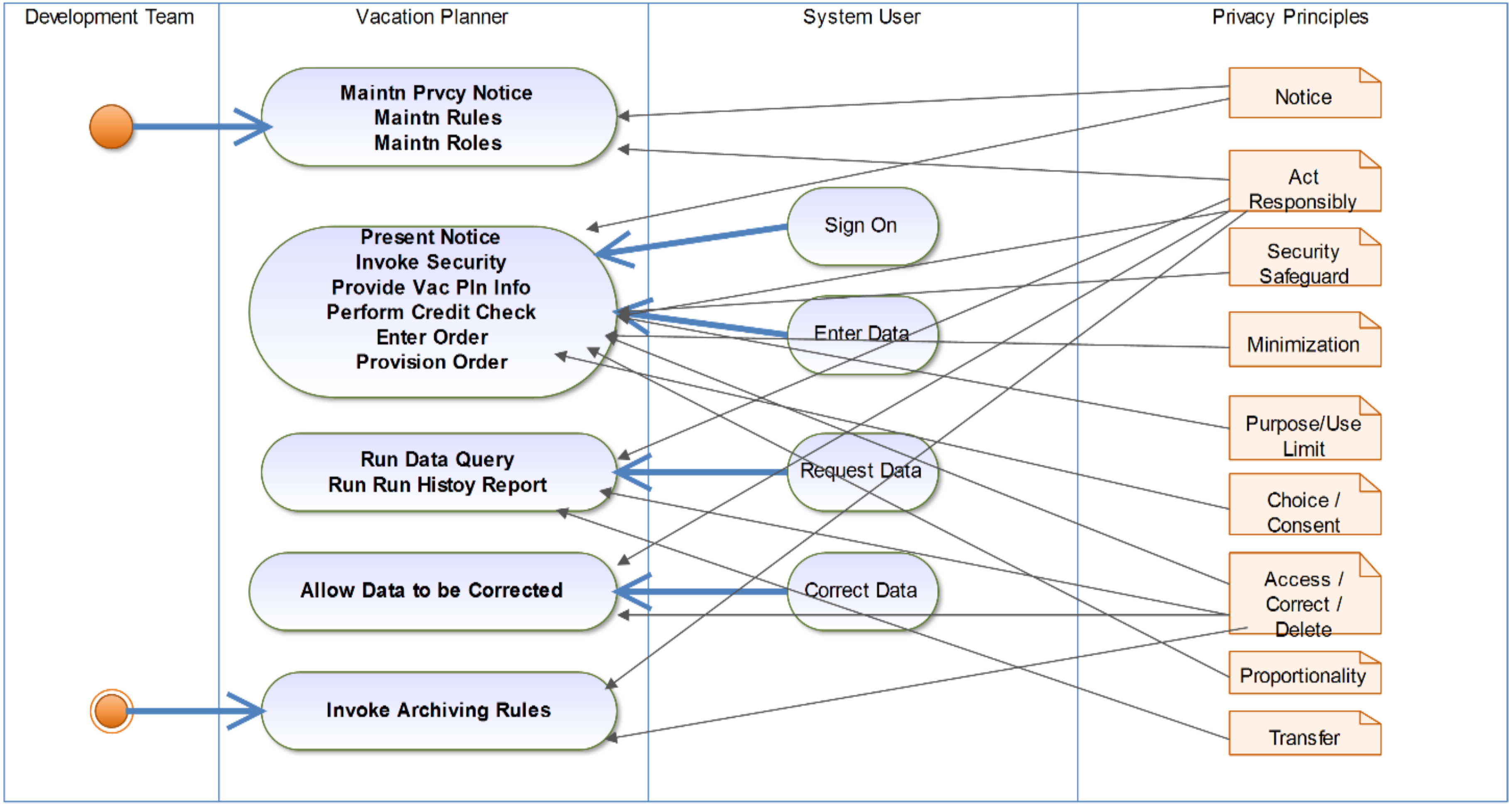
Account
Acct ID
Addr ID

Order Payment
Order ID
Acct ID
Payment ID
Credit Appvl Ind

Shipping Order
Order ID
Shipping Trk
Acct ID
Addr ID

Employee
Employee ID

System Activity Diagrams as privacy tools



FIPPS and GAPP Distilled and actionable

- To get sufficient answers about product, system, process, or application, the following list of areas must be delved into and explored.
  - Data: What data is involved? Are they sensitive? Are they proportional? Do they constitute the minimum necessary?
  - *Purpose:* How and why is the data being processed? Is the data being collected in alignment with the services for which the data is being collected? Is the need and reason for each data element documented?
  - *Means of collection:* How was the data acquired? From the individual? From another system? From a third party? Were they legitimately collected with notice and choice?
  - *Notice:* Where was notice presented? What was in the notice? Did it adequately explain how the personal information would be processed? Was it a just-in-time notice or via a link to a privacy notice?
  - *Choice/Consent:* What kind of choice is the owner of the data given? Is the use of the data an option? Is consent to process the personal information required? If check boxes were used, was there a prechecked box?
  - *Transfer:* Is it possible to transfer the data to third parties or another system? For what and whose purpose? Are contracts in place with the third parties? Has a privacy review been conducted? Is the data protected during transfer? Are there cross-jurisdictional issues?

FIPPS and GAPP Distilled and actionable

- *Access, Correction, Deletion:* Does the user have a means of accessing his or her personal information and the ability to correct or delete it should it be false or inaccurate? How is the data segmented to facilitate this? Is it a self-service model? Is there a process documented and tested?
- *Security:* Is the data secure at rest or in motion? Are both required? Is the means of authentication and authorization process sufficient? Is the security mechanism overly invasive?
- *Minimization:* Is the data collected the minimum necessary to achieve the intended purpose? Has the data passed the "minimization test" (as discussed earlier in this chapter)?
- *Proportionality:* Is the processing of the data proportional to the need, purpose, and sensitivity of the data? If the purpose of the processing were to be reported in the media, would it be "embarrassing" to the enterprise?
- *Retention:* Is the deletion strategy defined and enforced within the system or the enterprise? If so, how?
- *Third parties:* If third parties are involved, what is the relationship? Has a contract been signed? What is in the contract? Is a separate PIA required? Has a security review of the third party been completed?
- *Accountability:* Are responsibilities defined and the internal enforcement mechanisms in place? What are they? Who "owns" the program? How is it managed?

intel® Security