Demystifying Privacy by Design

Stuart Shapiro

Julie Snyder

MITRE

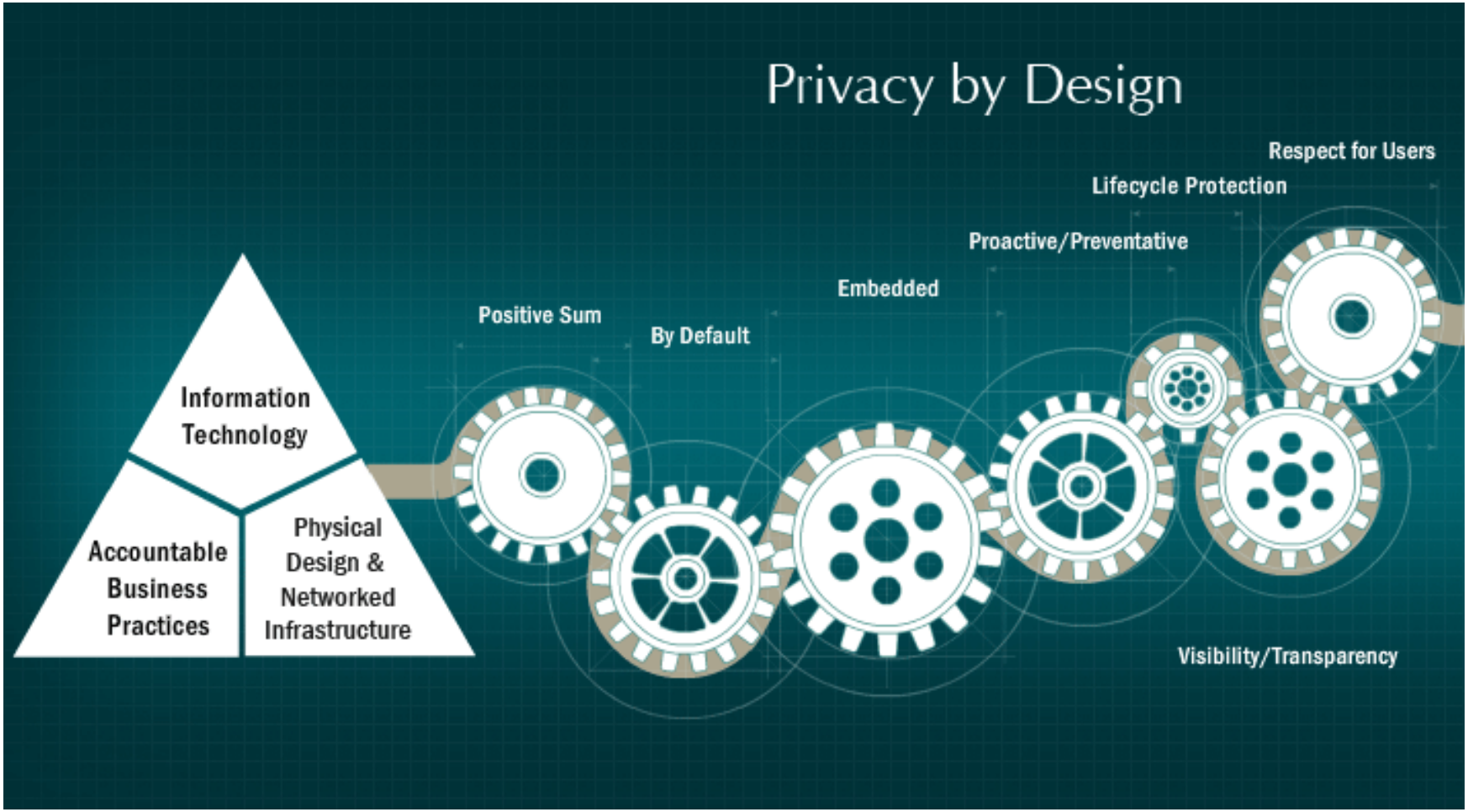
Overview

- Diagnosis
- Treatment
- Prognosis

Diagnosis

MITRE

Privacy by Design (PbD)



http://www.privacybydesign.ca/

7 Foundational Principles

1. ***Proactive*** **not Reactive;** ***Preventative*** **not Remedial**
2. **Privacy as the** ***Default Setting***
3. **Privacy** ***Embedded*** **into Design**
4. **Full Functionality — *Positive-Sum*, not Zero-Sum**
5. **End-to-End Security — *Full life cycle Protection***
6. ***Visibility*** **and** ***Transparency*** **— Keep it *Open***
7. ***Respect*** **for User Privacy — Keep it *User-Centric***

http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf

Now what?

The PbD Gap: Systematically Getting from A to B

- Absence of methodology
- Absence of an explicit risk model
- Problematic implicit risk model

What Many Organizations are Doing

- **Renewed focus on:**
  - Policy
  - Risk assessments (PIAs)
  - Notice
  - Records management
  - Accounting of disclosures
- **Data flow mapping**
- **Data loss prevention**
- **Metrics**
- **Waiting for Appendix J to save the day**

Google's Privacy Principles[1]

1. Use information to provide our users with valuable products and services.
2. Develop products that reflect strong privacy standards and practices.
3. Make the collection of personal information transparent.
4. Give users meaningful choices to protect their privacy.
5. Be a responsible steward of the information we hold.

[1] http://maps.google.com/intl/en/policies/technologies/

Google's Approach with Street View

- **Shoot (Street View footage) first, ask questions later**
  - While courts across the globe (both judicial and public opinion) beat you up….
- **Make smarter decisions only after required by the courts**

[2] http://maps.google.com/help/maps/streetview/learn/where-is-street-view.html

MITRE

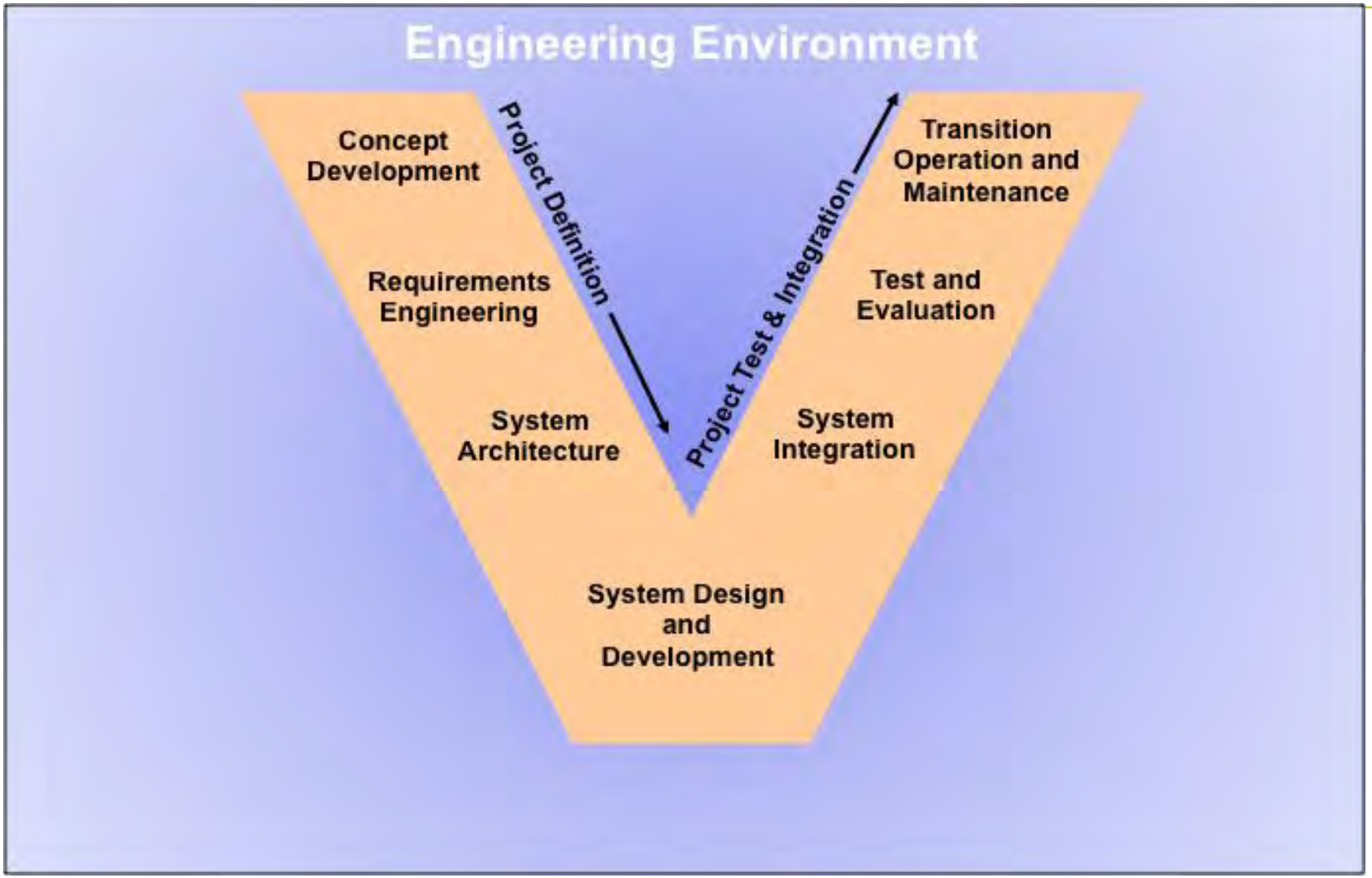
Treatment

MITRE

A Systems Engineering Definition of PbD

- **A systematic process for defining and implementing requirements for addressing privacy risks within the systems engineering life cycle**
  - Privacy requirements ultimately must be defined with sufficient precision that they can be readily translated into implementable system functionality and properties
  - A risk-driven process must be supported by a sufficiently comprehensive risk model

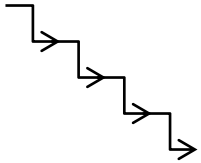
Systems Engineering Life Cycle



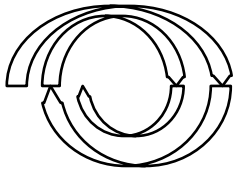
MITRE

Life Cycle Variants and Invariance

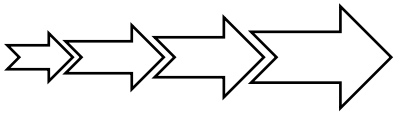
- **Nature of the activities tends to be invariant but location and timing will vary by life cycle type**
- **Waterfall**



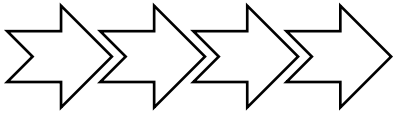
- **Spiral**



- **Prototyping**



- **Agile**



Requirements Engineering/Definition

- **Functional vs. “non-functional”**
- **Baseline vs. bespoke**
- **Business model vs. functional model**
- **Risk analysis**
  - Multiple possible non-exclusive risk models
    - Compliance
    - Fair Information Practice Principles (FIPPs)
    - Nissenbaum’s contextual integrity heuristic
    - Solove’s taxonomy of privacy harms
    - Others
  - Hybrid model
    - FIPPs
    - Contextual integrity disruptions => vulnerabilities
    - Exploited vulnerabilities => harms

Privacy Requirements Definition for Google Street View

"Google Maps with Street View lets you explore places around the world through 360-degree street-level imagery. You can explore world landmarks, view natural wonders, navigate a trip, go inside restaurants and small businesses - and now even hike the Grand Canyon!"

Risk-Based Privacy Requirements

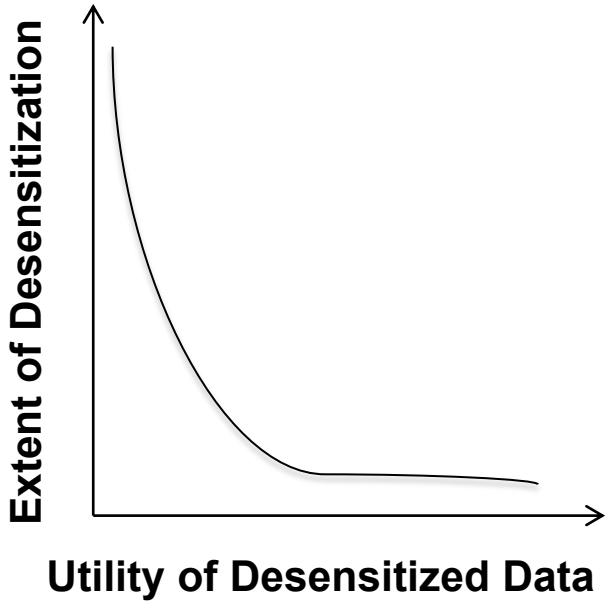
- **Aggregation => Problematize placement of identifiable people and things at a specific location**
- **Exposure => Mitigate potential future risk to individuals and other entities**
- **Increased accessibility => Reduce effective breadth of access to visuals of individuals and activities**

Baseline Privacy Requirements

- **The system shall only collect and use PII relevant to its purposes**
- **PII entering the system from other systems shall be limited to predetermined data elements**
- **Views of PII shall be defined for each distinct user and/or target system role**
- **All instances and formats of each PII data element shall be locatable and shall be deleted when any one instance of that PII is deleted.**
- **The system's intake of PII shall be consistent with the privacy notices related to the system and notices provided at points of collection**

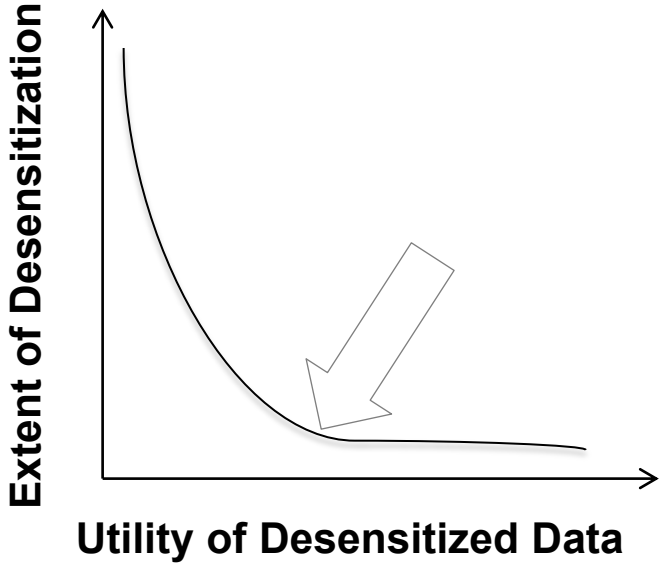
System Design and Development

- Data models
- Process models
- Design patterns
- Trade-off analysis



System Design and Development for Google Street View

- **Risk-based requirements**
  - Problematize placement of identifiable people and things at a specific location
  - Mitigate potential future risk to individuals and other entities
  - Reduce effective breadth of access to visuals of individuals and activities
- **Control options**
  - Anonymize location
  - *Anonymize people and things*
    - Automatically blur faces and vehicle license plates
    - Idiosyncratic residual risk



System Design and Development for Google Street View (cont.)

- **Baseline requirements**
  - The system shall only collect and use PII relevant to its purposes

    => Camera application shall only collect digital 360-degree images with meta-data containing location information from GPS coordinates and cellular towers
  - PII entering the system from other systems shall be limited to predetermined data elements

    => Back end interface shall only request image files from the Street View image store that have been scrubbed of individual identifiers.

    => Web server shall only receive meta-data fields containing location information from GPS coordinates and cellular towers
  - Views of PII shall be defined for each distinct user and/or target system role

    => Public web users (i.e. “everyone”) shall only have access to scrubbed images
  - All instances and formats of each PII data element shall be locatable and shall be deleted when any one instance of that PII is deleted

    => When individuals request an image with their PII be deleted, search all image files in-country on all image servers
  - The system's intake of PII shall be consistent with the privacy notices related to the system and notices provided at points of collection

    => Image capture dates shall be consistent with information posted on the “Where our cars are currently driving” site

Test and Evaluation / Verification and Validation

- Verification vs. validation
- Executable tests
- Reviews

Test and Evaluation for Google Street View

Requirement	Sample Test	PbD Result	Street View Result
The system shall only collect and use PII relevant to its purposes.	Review system data model and database architecture and associate each PII data element or logical aggregate of elements (e.g., mailing address) with a rationale for its inclusion.	**PASS** Data model and database architecture for camera application both reflect image file meta-data that only contains GPS coordinates and cellular towers with clear documentation for need and appropriate configuration of technologies to capture only the specified meta-data.	**FAIL** Documentation reflects: • Data model and database architecture consistent with stated purpose • Use of technologies that capture more information than intended

Test and Evaluation for Google Street View

Requirement	Sample Test	PbD Result	Street View Result
PII entering the system from other systems shall be limited to predetermined data elements.	Review interfaces to verify PII data elements being requested.	**PASS** Back end interface only requests images scrubbed of identifiers.	**FAIL** Back end interface requests original images with all metadata, which includes WiFi router information captured by the camera application (e.g. SSID, encryption type).
	Review interfaces to verify PII data elements being received.	**PASS** Web server only receives image location meta-data for GPS Coordinates and cellular towers.	**FAIL** Interfaces are not limited to image files and location from GPS and cellular towers – also capturing wireless router SSIDs and traffic (e.g. emails, passwords, photos).

Test and Evaluation for Google Street View

Requirement	Sample Test	PbD Result	Street View Result
Views of PII shall be defined for each distinct user and/or target system role.	Log into the system as test users with differing roles to verify that viewable PII is consistent with roles.	**PASS** Public user roles are only able to see scrubbed images with all PII blurred.	**FAIL** Public user roles can see clear photos of faces, license plates, and other identifying information.
All instances and formats of each PII data element shall be locatable and shall be deleted when any one instance of that PII is deleted.	Load test input data so as to produce multiple instances of processed PII. Initiate processing and deletion, then manually query the database for the presence of each instance of PII.	**PASS** No images with specified PII (e.g. easily identifiable clothing, unique tattoo, car detailing/paint job) found.	**FAIL** All copies of image in question removed, but other images found with the same PII (e.g. facial image, license plate).

Test and Evaluation for Google Street View

Requirement	Sample Test	PbD Result	Street View Result
The system's intake of PII shall be consistent with the privacy notices related to the system and notices provided at points of collection	Compare documented system inputs with relevant privacy notices.	**PASS** Image capture dates align with locations published on the "Where our cars re currently driving) site.	N/A – Google didn't believe a notice was required (Public is public!).

Test and Evaluation for Google Street View

The "Big Picture" Takeaways from Test and Evaluation:

- **We're getting more information than we need to meet the purpose of Street View**
- **We're getting information people may find sensitive (who was where and when)**
- **We may not be able to effectively delete everything**
- **We need to think about privacy notices**
- **We need to figure out what privacy rules apply**

Where We Ended Up vs. Where Google Ended up

Street View Privacy Features[3]:

- Public access only
- Images are not real-time
- Individuals and license plates are blurred

Additional Features[3,4]:

- Request process for additional blurring and removal of images
- Publish a list of where Street View cars are currently driving

Us:

- Determine jurisdictional privacy posture during concept phase
- Provide advance notice
- Remove objectionable images
- Pixelate faces, license plates and other identifiable images with X% accuracy
- Collect only the minimum information necessary to link a photo to a specific location with X-degree of certainty
- Destroy original images after product Street View image is produced/X retention period

[3] http://maps.google.com/help/maps/streetview/privacy.html

[4] http://maps.google.com/help/maps/streetview/learn/where-is-street-view.html

Prognosis

MITRE

Opening the Engineering Black Box

- **Doing Privacy by Design necessitates treating the engineering process as something other than a black box**
  - Privacy by Requirements
  - Privacy by Testing
- **Doing privacy reviews, including privacy impact assessments, is all well and good, but it's not**
  - Engineering
  - Likely to integrate privacy into a socio-technical system
    - Systematically
    - Comprehensively

Privacy *is* Different But not *that* Different

- **So are**
  - Security
  - Usability
  - Reliability
  - Efficiency
  - Etc.
- **Distinctiveness does not imply SELC incompatibility**

- **Specialized frameworks and methods exist for working with all these properties *within the SELC***
- **These are needed for privacy as well**

Questions & Contacts

Stuart Shapiro
sshapiro@mitre.org
(781) 271-4676

Julie Snyder
jsnyder@mitre.org
(202) 491-1500

MITRE