# Privacy Engineering Training

Frank Dawson
(frank dot dawson at Nokia dot com)

2013-06-14

Consumer privacy issues are a Red Herring.
You have zero privacy anyway,
*so get over it!*

Scott McNealy, CEO Sun Microsystems
(Wired Magazine Jan 1999)

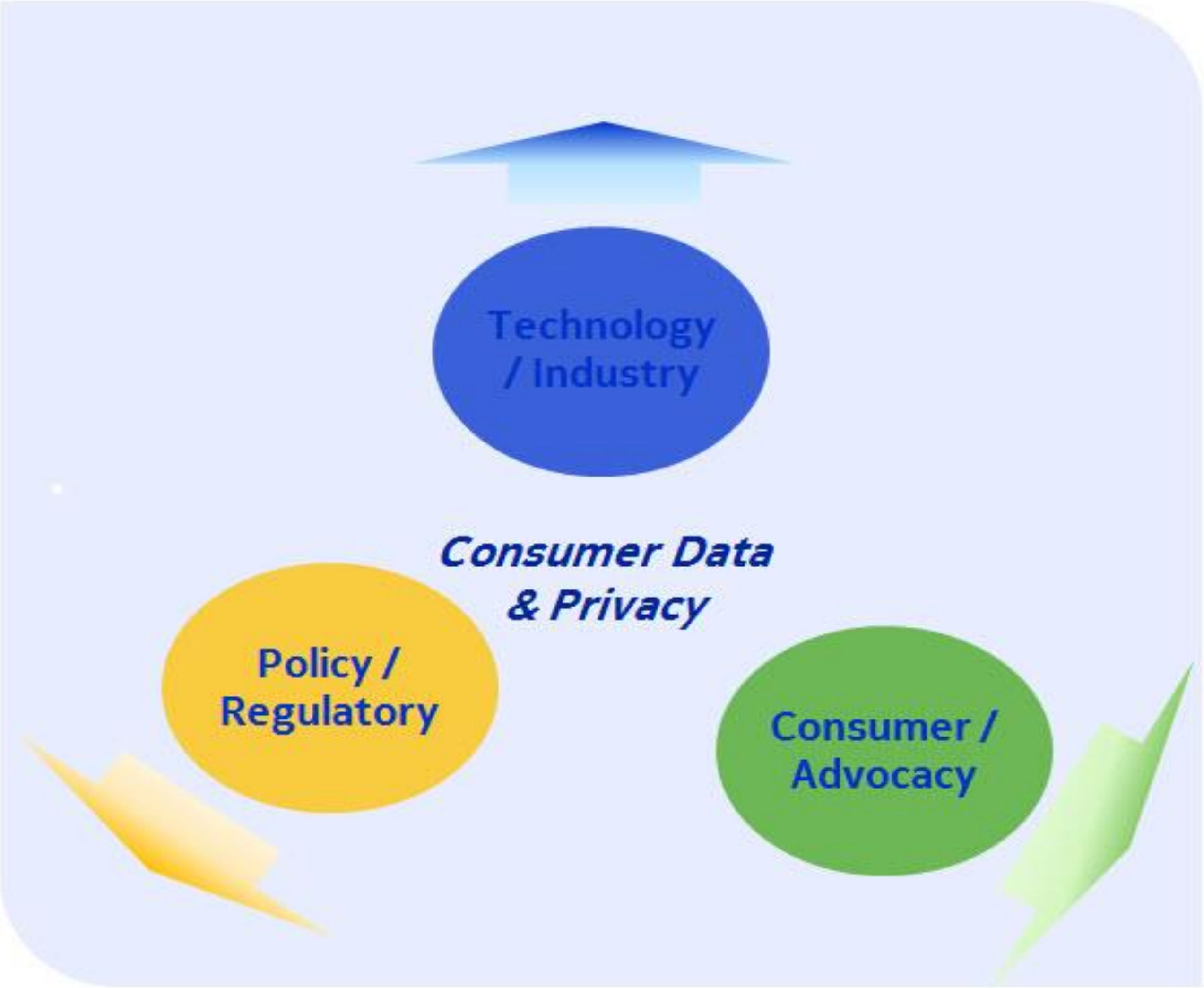
WIRED
Quick! The future is all about>>> people
William Gibson Reveals His Secret eBay Obsession
The Truth About Vibrators
Daytrading: The Net's Extreme Sport
Phone Sects: What Happened When the Amish Went Wireless
Salon's Web Dream

# Contents

- Privacy contexuality
- **WHY** – Imperative for privacy
- **WHAT** – Defining the privacy intent for a project
- **WHAT** - Information privacy
- **HOW** - Privacy engineering
- Privacy compared to security

# Privacy Contextuality

# Privacy triangle of trust



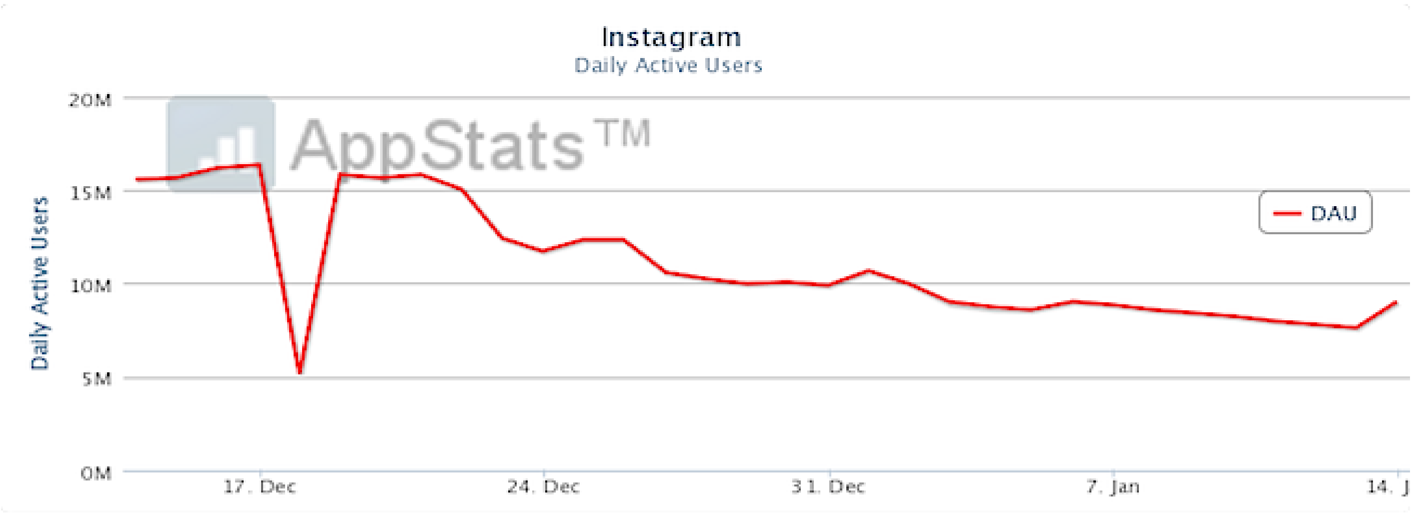
# WHY
# Imperative for Privacy

# 2013

Instagram case

- Facebook owned photo sharing social network site proposed changing its terms of use so it could exploit members' photographs for profit - without compensating the owners
- Impact: Daily active users fell from almost 16.3 to about 7.6 million
- Brand damage: ”To do a Zuckerberg” and ”To be Instagrammed” coined

- Principles violated: Fair-Value Exchange, Proportionality

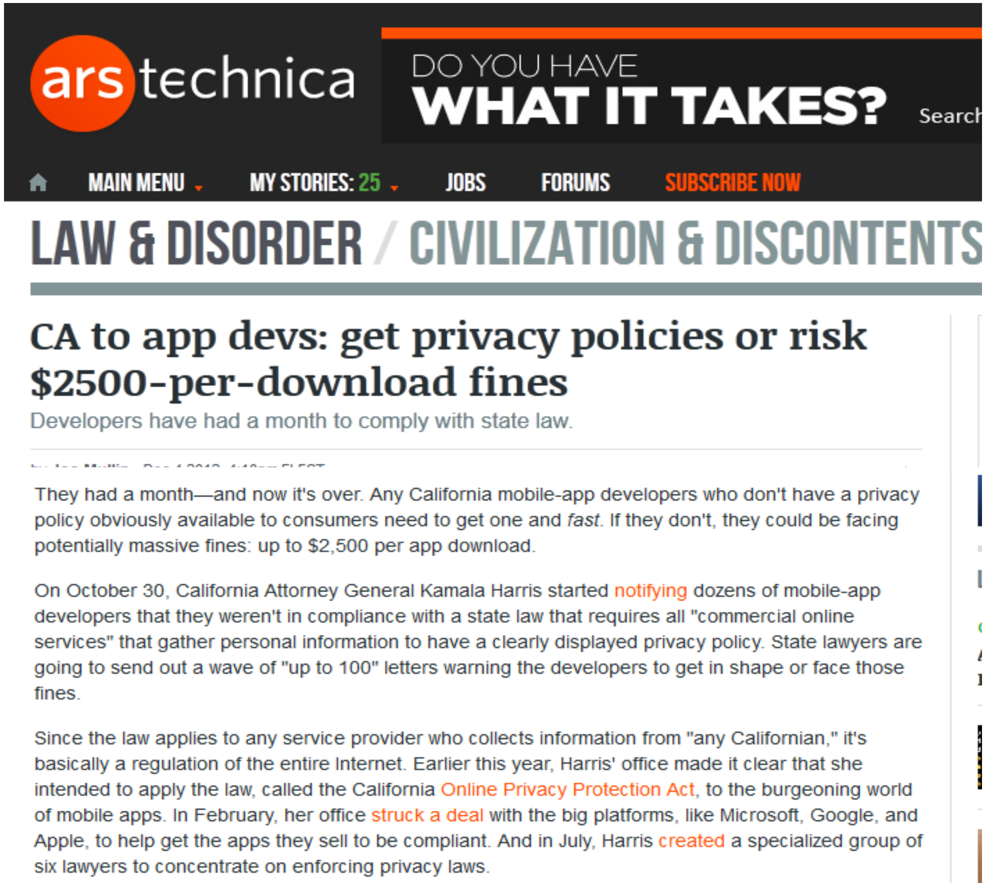


# 2012

Delta mobile app case

- US: CA AG warned mobile apps developers they had 30 days to provide consumer with privacy policy prior to download
- Delta Airline provided frequent flyers with mobile app missing a privacy policy
- Fine: USD$2500 per mobile download, est. +30M SkyMiles members

- Principles violated: Transparency, Choice, Consent


ars technica
DO YOU HAVE WHAT IT TAKES?
Search
MAIN MENU
MY STORIES: 25
JOBS
FORUMS
SUBSCRIBE NOW
LAW & DISORDER / CIVILIZATION & DISCONTENTS

## CA to app devs: get privacy policies or risk $2500-per-download fines

Developers have had a month to comply with state law.

by Joe Mullin - Dec 4 2012, 4:10pm EST

They had a month—and now it's over. Any California mobile-app developers who don't have a privacy policy obviously available to consumers need to get one and *fast*. If they don't, they could be facing potentially massive fines: up to $2,500 per app download.

On October 30, California Attorney General Kamala Harris started notifying dozens of mobile-app developers that they weren't in compliance with a state law that requires all "commercial online services" that gather personal information to have a clearly displayed privacy policy. State lawyers are going to send out a wave of "up to 100" letters warning the developers to get in shape or face those fines.

Since the law applies to any service provider who collects information from "any Californian," it's basically a regulation of the entire Internet. Earlier this year, Harris' office made it clear that she intended to apply the law, called the California Online Privacy Protection Act, to the burgeoning world of mobile apps. In February, her office struck a deal with the big platforms, like Microsoft, Google, and Apple, to help get the apps they sell to be compliant. And in July, Harris created a specialized group of six lawyers to concentrate on enforcing privacy laws.

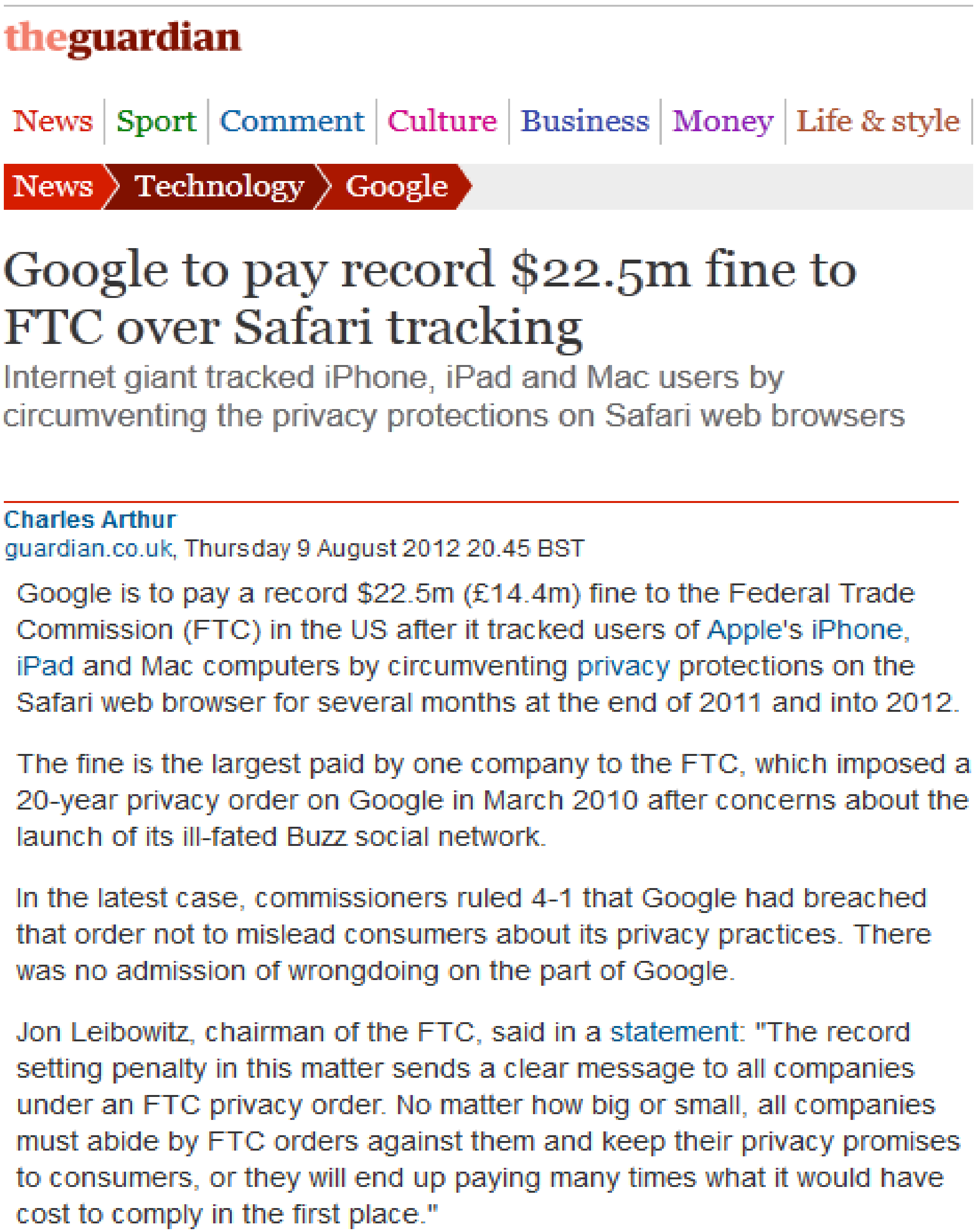
# 2012

Google tracking case

- Circumvented Apple privacy safeguards on Safari browsers
- Stanford research discovers DoubleClick over-riding cookie control
- Millions of consumer effected

- FTC imposes record fine
- Prompts EU investigations

- Principles violated: Transparency, Consent, Fair & legal, Legitimate purposes



## Google to pay record $22.5m fine to FTC over Safari tracking

Internet giant tracked iPhone, iPad and Mac users by circumventing the privacy protections on Safari web browsers

Charles Arthur
guardian.co.uk, Thursday 9 August 2012 20.45 BST

Google is to pay a record $22.5m (£14.4m) fine to the Federal Trade Commission (FTC) in the US after it tracked users of Apple's iPhone, iPad and Mac computers by circumventing privacy protections on the Safari web browser for several months at the end of 2011 and into 2012.

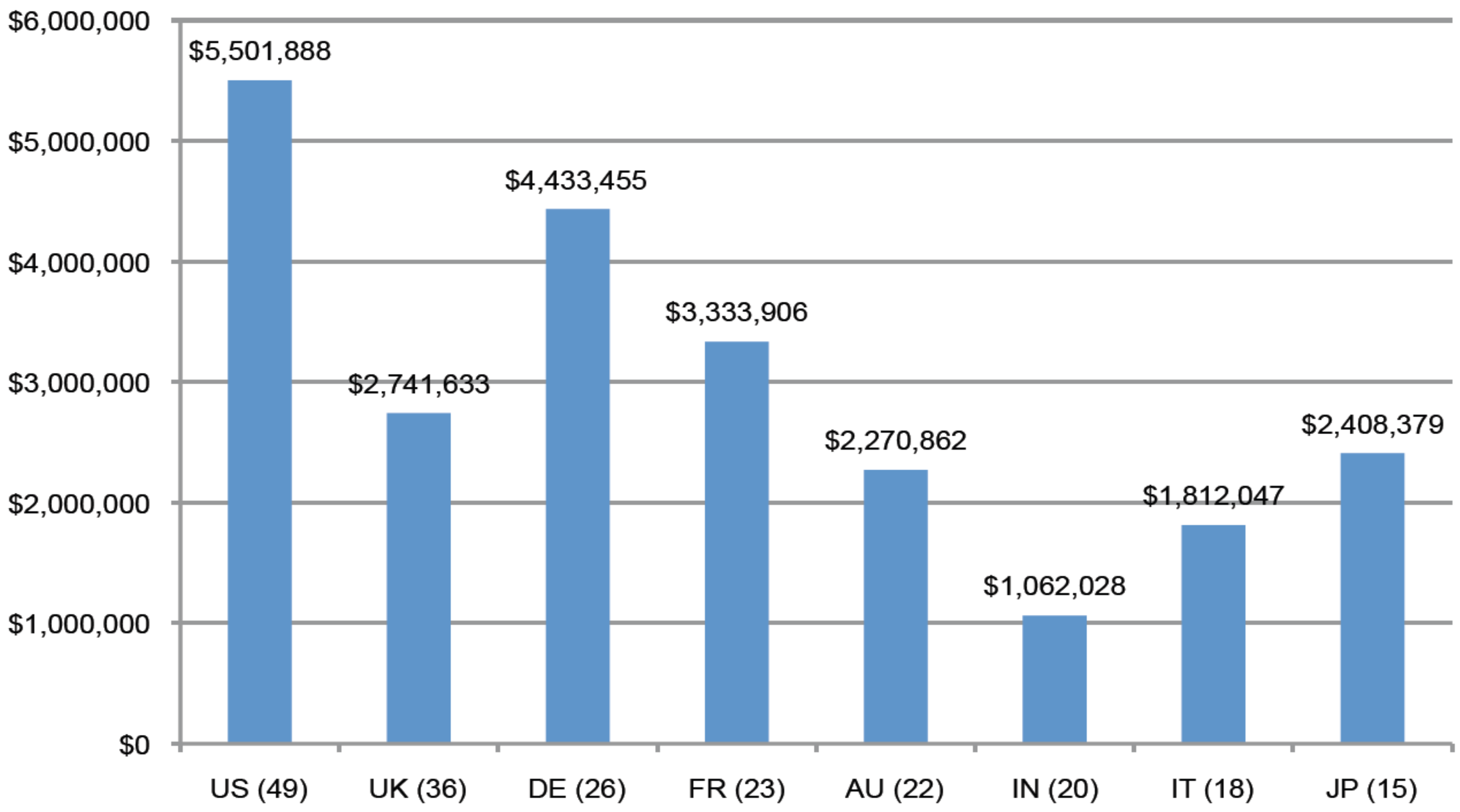
The fine is the largest paid by one company to the FTC, which imposed a 20-year privacy order on Google in March 2010 after concerns about the launch of its ill-fated Buzz social network.

In the latest case, commissioners ruled 4-1 that Google had breached that order not to mislead consumers about its privacy practices. There was no admission of wrongdoing on the part of Google.

Jon Leibowitz, chairman of the FTC, said in a statement: "The record setting penalty in this matter sends a clear message to all companies under an FTC privacy order. No matter how big or small, all companies must abide by FTC orders against them and keep their privacy promises to consumers, or they will end up paying many times what it would have cost to comply in the first place."

# Average cost of unauthorized disclosure

Figure 2. The average total organizational cost of data breach



Source: http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-global.en-us.pdf

# Why is *privacy* important?

✓Authorities are doing joint-enforcement on major companies

***Example***: Facebook

➢Canadian, US, Nordic, Irish regulators investigated complaints and found violations

✓Increasing public policy maker interest in mobile technologies

***Example:*** Positioning technologies

➢More and more laws globally

*Enforcement Actions:*

€ Fines

€ Penalties

€ Cost of remediation

€ Forced privacy program

€ 20 year external audit

€ Deletion of unlawfully collected data

€ Sales stops, recalls

# WHAT
# Setting the Privacy Context

# Compliant versus Accountable

- Today, it is nolonger sufficient to just be compliant but companies are being tasked to show that they are accountable to our privacy goals

- Implications to your project include:
    - Identify your information privacy team
    - Get awareness and education training for the team
    - Specialty training for added key team members
    - Privacy champ is identified in the product team
    - ***Products need a privacy assessment sign-off***
    - Proper and timely handling of operational issues

# Elements of an Accountable privacy program

## 1. Executive Accountability and oversight

✓Internal senior executive oversight and responsibility for data privacy and data protection

## 2. Policies  and processes to implement them

✓Binding and enforceable written policies and procedures that reflect applicable laws, regulations and industry standards, including  procedures to put those policies into effect

## 3. Staffing and delegation

✓Allocation of resources to ensure that the organization's privacy program is appropriately staffed by adequately trained personnel

## 4. Education and awareness

✓Existence of up-to-date education and awareness programs to keep employees and on-site contractors aware of data protection obligations

## 5. Risk assessment and mitigation

✓Ongoing risk assessment and mitigation planning for new products, services, technologies and business models.

✓ Periodic Program risk assessment to review the totality of the accountability program

## 6. Event management and complaint handling

✓Procedures for responding to inquiries, complaints and data protection breaches

## 7. Internal enforcement

✓Internal enforcement of the organization's policies and discipline for non-compliance

## 8. Redress

✓Provision of remedies for those whose privacy has been put risk

*Not just compliant but accountable*

# Role of the information privacy team

- Creating lead technical roles within an organization with responsibility for implementation and assurance that privacy is accounted for during the product development lifecycle is critical element of Accountability

- Forms basis for the operational component of an organization’s privacy program

- These roles include one or more Unit Privacy Officers and Privacy Champs across the organization’s various business units

- General responsibilities focus on goal of advocating Privacy by Design principles in product teams through implementation and assurance activities related to privacy safeguards in an organization’s products and service

- Also shapes future choices in information privacy technologies by participating in industry collaboration and in-house technology road mapping projects

# Unit privacy officer

- Responsibility and oversight for timely and proactive support to ensure Privacy by Design followed within the development lifecycle of products and services
- Monitors and reports on privacy compliance status to accountable executive for privacy wihtin the organization
- Creates and supports a network of Privacy Champs within product teams
- Acts as a subject matter expert for specific information privacy competence areas and resources
- Organizes and conducts privacy training & awareness  within the organization
- Participates in identifying privacy risks and technical supportt of issue response management
- Contributes to the overall organizational privacy program (E.G., Privacy vision, Privacy policy, Privacy principles, Privacy safeguarding requirements, Privacy engineering processes)

# Privacy champ

- Role description is adjusted to product resourcing levels
- Typically staffed from within product team
- In-depth understanding of privacy requirements and ability to apply understanding to one’s own responsibility area
- Understand privacy requirements and represent privacy views inside own team/organization/responsibility area and interpret what the requirements mean in the context of own responsibility area
- Contribute to Privacy Impact Assessments, threat analysis
- Collaborates with other privacy champs

# Define the privacy intent for the product

- Vision: Articulates the high level aspirations to protecting the personal data of individuals using the product
  - E.G., ”Consumers trust us to meet their privacy expectations”

- Principles: Identify which privacy principles apply to the product
  - E.G., select from those codified in OECD, FIPP, EU frameworks

- Objectives and activities: Define concrete objectives and related activities to achieve the objectives
  - E.G., Industry leading privacy controls built into our software by adopting Privacy by Design,
  - E.G., Mature privacy aware culture through training and effective governance and processes

# Privacy related processes

## Issue Response Management (IRM)

- Ensures that alleged and reported issues or incidents treated properly

## Privacy Breach

- Deals with alleged unauthorized access to, or collection, use or disclosure of personal data and describes the actions that need to be taken in the case of a privacy breach

## Authority Request

- Deals with requests by authorities for personal data

## Consumer Request

- Ensures timely response to consumer requests to exercise their rights E.G. access to their personal data or to delete or modify unnecessary, incorrect or outdated personal data

# WHAT
# Information Privacy

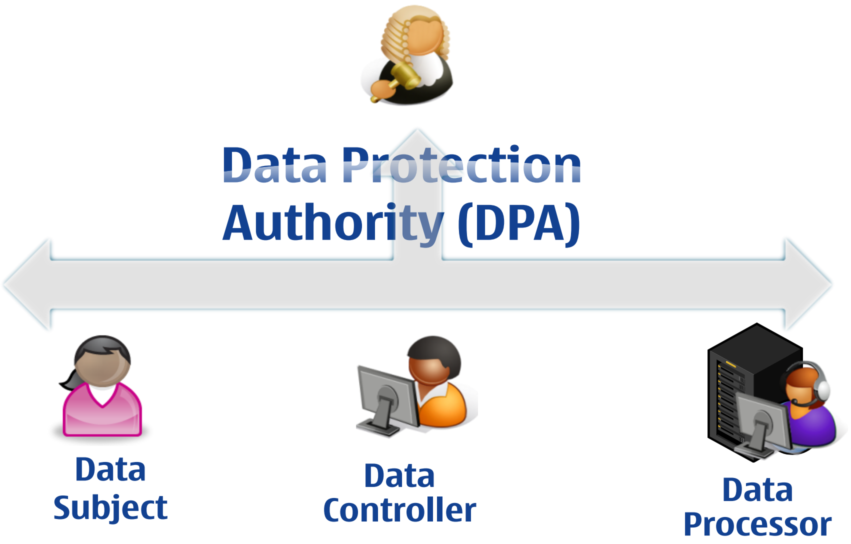
# Privacy theorem

- Privacy impact equation
  - **PD = Fn (Pi, In)**
  - Privacy impact is a function of the personal information and information nymity associated the system or specification under reviewed (SUR)
- Identifiability equation
  - **IN = Fn (Id, Lk, Ob)**
  - Identifiable is a function of the identifiability, linkability and observability character of the data within the SUR, establishes the ”nymity” component of PII
- Threat equation
  - **$TH = \Sigma_{pd=1..n}(Fn(Pl_i, Pp_i, Th_i, Ps_i))$**
  - Threat is a function of sumation for each personal data, of the tuples of the privacy data lifecycle context, associated privacy principle, identified threat and specific privacy safeguard applied in the SUR
- Risk equation
  - **$RK = \Sigma_{th=1..n}(Fn(Tt_i, Hm_i, Hp_i, Rm_i))$**
  - Risk is a function of the sumation of the tuples of the threat type, harm magnitude, harm probability and risk mitigation applied in the deployment of the SUR

***REALITY CHECK: Privacy cannot yet be simplified into a few equations but this could become the future, if Privacy Engineering matures into a technolical discipline***

# Roles within the privacy framework

- DPA, Data Privacy Authority, Information Privacy Commissioner, etc. is the independent legal authority for administering privacy rules within a country
- The consumer is the Data Subject
- The Data Controller is entity that determines purposes and means of processing consumer's personal data
- The Data Processor performs information processing on behalf of the Data Controller



*Sometimes a reference is also made to a Third Party, which can be viewed as outside this privacy framework, but the responsibility of the Data Controller.*

# Personal data/information

- Personal information relates to information about a natural person
- When the data can be associated with an individual, it is referred to as Personally Identifiable Information (PII)
- Criteria for linkability of data to an individual is a hot-topic within the privacy community
- Sensitive PII must be treated specially
- Generally, if PII is of a racial, religious, political, sexual orientation, medical nature, it is characterized as Sensitive; but other categories should also be consisted
- Also commonly referred to as Personal Data

*Basic data (E.G. first name, last name, mobile number)*

*Address data (E.G. postal code, email address)*

*Restricted categories of data (E.G. racial or ethnic origin, religion, trade union membership – if allowed by applicable law)*

*Social networking related data (E.G.. metadata of pictures uploaded, site activity information)*

*Location data (E.G. GPS coordinates or mobile network base station ID)*

*Identifiers (E.G. IMEI, device identifiers, IP-address)*

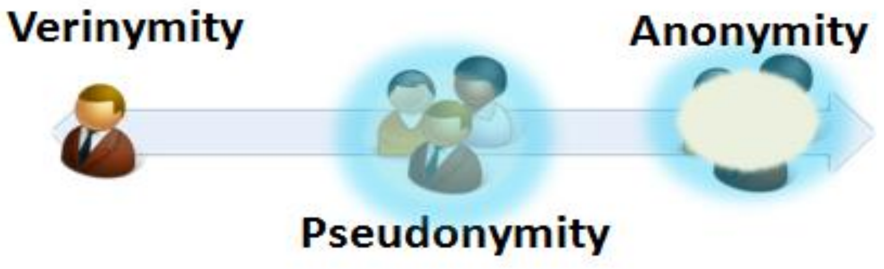
*Information on how individual users are using the system (E.G. log files)*

*Monetary transactions (E.G. credit card number, account information)*

These are some of the categories of personal data to consider when identifying the PII in your particular project

# Nymity

- The Theory of Nymity applies to the degree of identification; varying along a spectrum from full identity of the consumer to other extreme of no linkability to the consumer, at all
- Combinations of few characteristics often combine in populations to uniquely or nearly uniquely identify some individuals; leading some privacy advocates to doubt universality of anonymity
- *k-anonymous coefficient* is often referred to as a quantative measure of the linkability of data to an individual and a measure of the level of anonymity
- Best to treat all PII with appropriate privacy controls, because over time, addition of context can compromise current level of anonymity



# Measuring nymity – An analysis tool

- ***Identifiability***
  - A measure of degree which information is personally identifiable. The identity measurement takes place on a continuum, from full anonymity (the state of being without name) to full verinymity (being truly named)
- ***Linkability***
  - A measure of degree to which data elements are linkable to true name of the data subject, where unlinkability meant different records cannot be linked together and related to a specific personal identity. In this regard, complex interrelations have been taken into account, as it may be organized and/or made possible in different ways
- ***Observability***
  - A measure of the degree to which identity or linkability are affected by the use of a system. It considers, in fact, any other factor relative to data processing (time, location, data contents) that can potentially affect the degree of identity and/or linkability

# EU guidance on personal data

***Personal Data*** as defined by the Directive 95/46/EC (Article 2) 'shall mean *any information relating to an identified or identifiable natural person* ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity’. Additionally, WP 136 and WP 175 (section 2.2) of Art. 29 Data Protection Working Party should be considered, which detail the concept of personal data and qualify a unique number as personal data if it is carried by a person.

***Sensitive Personal Data*** is defined by the Directive 95/46/EC (Article 8) as any personal data that relates to (a) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject, (b) whether the data subject is a member of a trade union, (c) the physical or mental health or condition or sexual life of the data subject, (d) the commission or alleged commission of any offence by the data subject, or (e) any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings. Additionally, it is recommended to consider the context, too, when determining the sensitivity of personal data. Data that is not sensitive in itself may become sensitive in a specific context.

# Commonly referenced privacy principles

US FIPP

Notice/Awareness, Choice/Consent, Access/Participation, Integrity/Security, Enforcement/Redress (Self-regulation, Private remedies, Government enforcement)

OECD

Collection limitation, Data quality, Purpose specification, Use limitation, Security safeguards, Openness, Individual participation, Accountability

EU Directive 95/46/EC

Transparency, Legitimate purpose, Proportionality, Personal data, Processing, Data quality (Fair & legal, Purpose-limited, Relevant, Accurate, Time-limited), Legitimate data processing (Consent, Contract, Legal obligations, Vital interests, Public interest, Legitimate interests), Processing senstive information

EU-US Safeharbour

Notice, Choice, Onward transfer, Security, Data integrity, Access, Enforcement

ISO 29100/Privacy Framework

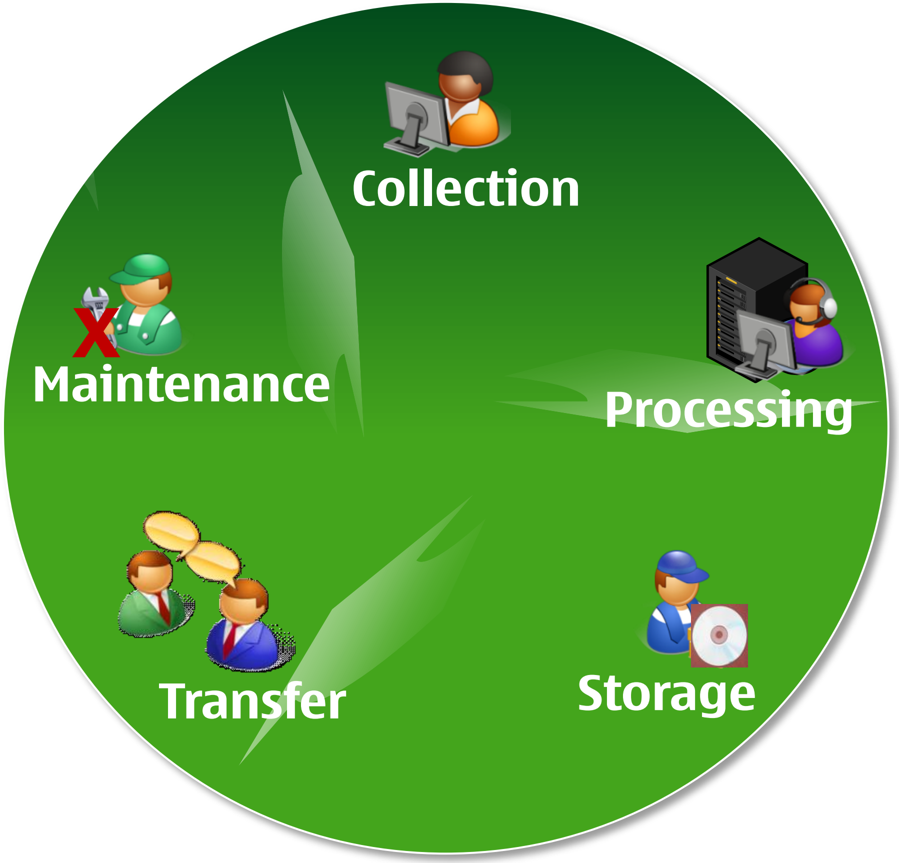
Consent & choice, Purpose legitimacy & specification, Collection limitation, Data minimization, Use & retention & disclosure limitation, Accuracy & quality, Openness & Transparency & Notice, Individual participation & access, Accountability, Information security, Privacy compliance

GSMA High Level Privacy Principles

Openness Transparencey and Notice, Purpose and Use, User Choice and Control, Data Minimization and Retention, Respect User Rights, Security, Education, Children and Adolescents, Accountability and Enforcement

# Privacy data lifecycle

- Also called the *Consumer Data Lifecycle* , it is a fundamental component of the privacy knowledge base
- Define the actions related to personal data within the privacy framework
- When analyzing the data flow in your specifications, you should also consider the complete lifecycle for the associated PII
- Within the EU, *collection*, itself is considered to be an act of *processing* !



# Privacy by Design, Accountability

- PbD
  - Bake-in privacy into specifications from the beginning, rather than retro-fit to existing specifications
  - Privacy by Re-Design (PbRD) is inevitable for legacy specifications
  - 7-Foundation 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 Lifecycle Protection
    6. Visibility and Transparency — Keep it Open
    7. Respect for User Privacy — Keep it User-Centric
  - Is now globally included into regulations
- Accountability
  - Do What You Say _and_ Demonstrate It!
  - Aim to achieve more than just compliance
  - Is now globally included into regulations

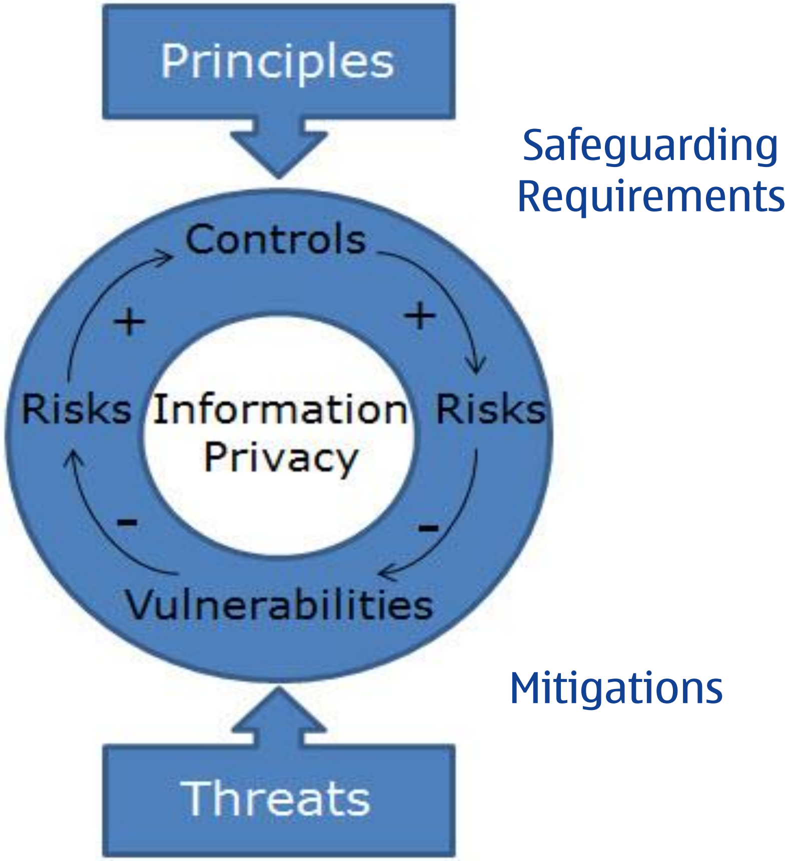
# HOW
# Privacy Engineering

# Privacy safeguards/controls

- ***Privacy Engineering*** is emerging as a discipline based on accepted information privacy concepts, processes and tools similar to those found in information security practices

- Based on a cycle formed by ***principles*** (and **safeguarding *requirements***), supported by technology ***safeguards*** or ***controls*** and dependent on iterative vigilance to mitigate inevitable underlying ***threats*** to inherent ***vulnerabilities*** with ascertainable ***risks***

- Control types include Physical, Procedural, Technical, Legal and/or Regulatory



*Ref: US/DoC NIST SP-800-53 Appendix J Privacy Control Catalog*

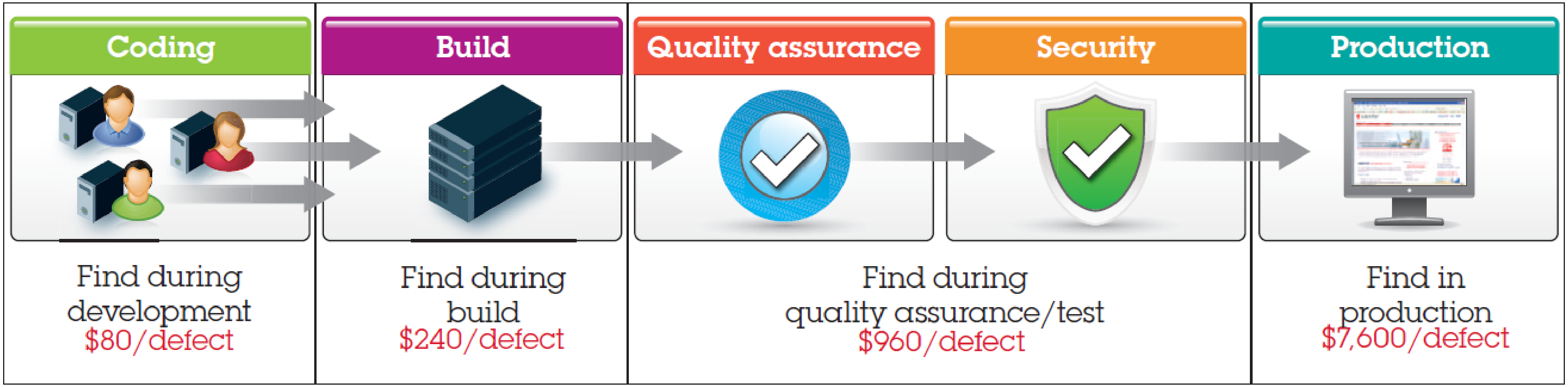
# Technical topics with privacy impact

- Internet protocols
- Internet and web formats
- Data schemas
- Web APIs
- Device APIs
- Web service definitions
- Browser plug-ins
- Proximity and connectivity standards for promoting data sharing, device coupling and service invocation
- Collaborative applications/services
- Device management services
- User experience and UI control
- Mobile applications and services

# Design principles that favor privacy

- Specification *Data Management* plan
- Data minimization
- Data security (confidentiality, integrity, availability) for personal data
- Clarity of purpose for data collection, use, storage, transfer, deletion (privacy data lifecycle)
- Limits on data retention
- Reduce the linkability of data with de-identification techniques
- Emphasis on complete product lifecycle
- Consumer centric privacy defaults

# Finding vulnerabilities early saves costs



Coding

Build

Quality assurance

Security

Production

Find during development $80/defect

Find during build $240/defect

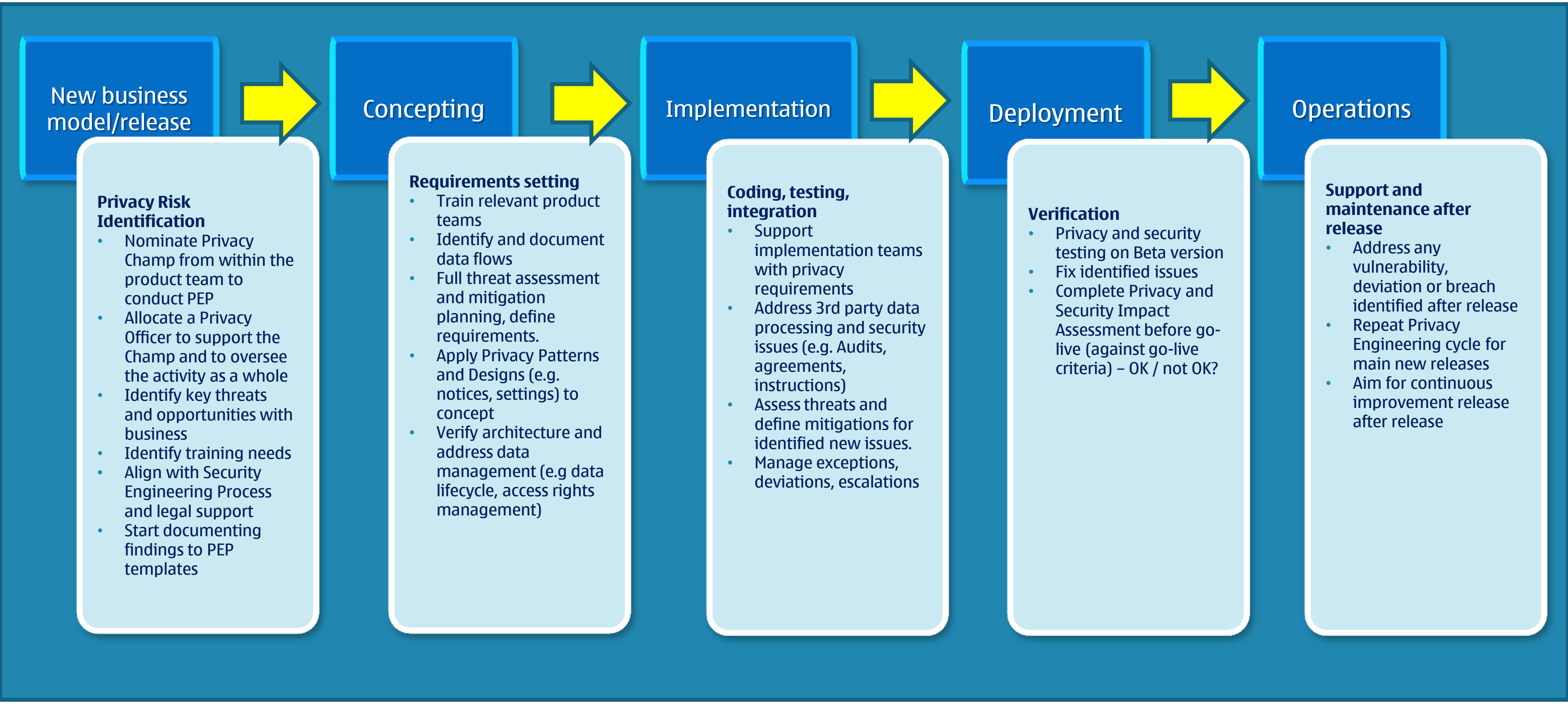
Find during quality assurance/test $960/defect

Find in production $7,600/defect

- While applicable to information security, this also applies to information privacy
- Identifying vulnerabilities early in the project lifecycle can prevent unnecessary costs when fixing security issues
- In this illustration the impacts are based on hypothetical cost basis but relative magnitude of cost escalation that occurs through the application lifecycle is typical of what IBM services experienced verified across many organizations

***Reference: "Five steps to achieve success in your application security program", IBM Whitepaper, http://searchsoftwarequality.bitpipe.com/detail/RES/1361993557_566.html, 2012.***

# Privacy Engineering Process (PEP)



New business model/release

**Privacy Risk Identification**
- Nominate Privacy Champ from within the product team to conduct PEP
- Allocate a Privacy Officer to support the Champ and to oversee the activity as a whole
- Identify key threats and opportunities with business
- Identify training needs
- Align with Security Engineering Process and legal support
- Start documenting findings to PEP templates

Concepting

**Requirements setting**
- Train relevant product teams
- Identify and document data flows
- Full threat assessment and mitigation planning, define requirements.
- Apply Privacy Patterns and Designs (e.g. notices, settings) to concept
- Verify architecture and address data management (e.g data lifecycle, access rights management)

Implementation

**Coding, testing, integration**
- Support implementation teams with privacy requirements
- Address 3rd party data processing and security issues (e.g. Audits, agreements, instructions)
- Assess threats and define mitigations for identified new issues.
- Manage exceptions, deviations, escalations

Deployment

**Verification**
- Privacy and security testing on Beta version
- Fix identified issues
- Complete Privacy and Security Impact Assessment before go-live (against go-live criteria) – OK / not OK?

Operations

**Support and maintenance after release**
- Address any vulnerability, deviation or breach identified after release
- Repeat Privacy Engineering cycle for main new releases
- Aim for continuous improvement release after release

***Activities across the product development lifecycle***

# PIA concept

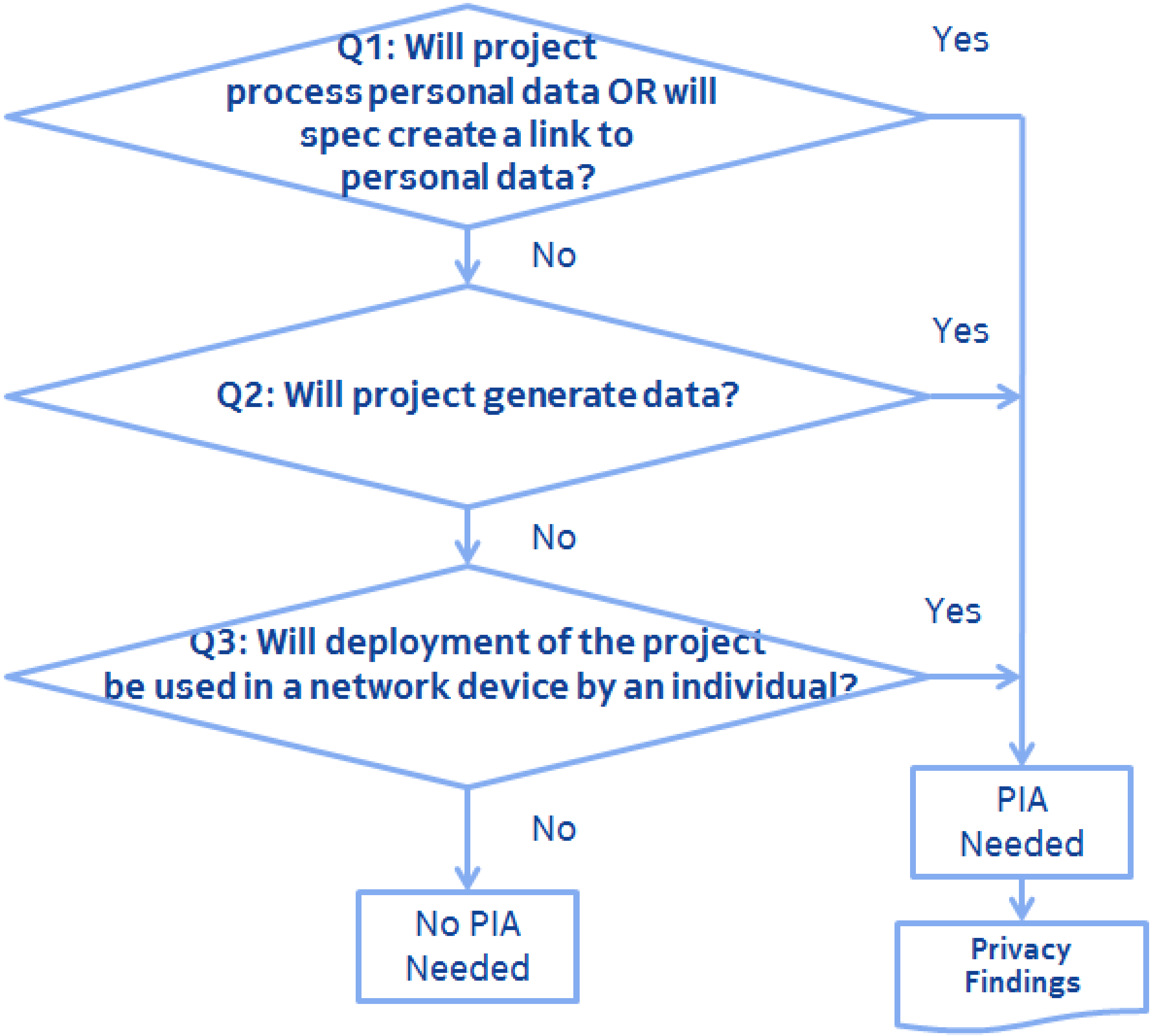
- **Privacy Impact Assessment** remains the common tool for implementing *Privacy by Design* in the product creation process
- Major component of the Privacy Engineering Process (PEP)
- Wraps together design analysis, threat analysis and risk analysis
- Should be undertaken by members of product team

- PIA concept consists of the following activities:
  1. Describing the product under review
  2. Capturing data flows between interactors;
  3. Classifying the associated personal data;
  4. Understanding the associated privacy principles;
  5. Identify inherent vulnerabilities that could threaten privacy;
  6. Adding privacy safeguards to mitigate identified threats;
  7. Working with product business team to analyze and mitigate likelihood of risks;
  8. Document findings as evidence of accountability within the product ; and
  9. Verify implementation of findings (results of analysis) regarding the product.

# Privacy engineering – tools of the trade

***Privacy Impact Assessment (PIA)***

- Methodology for analyzing project against applicable privacy principles, taking into account associated privacy safeguarding requirements and assessing potential threats that requirement mitigation with introduction of privacy safeguards/controls, based on risk assessment to harm caused by technology to consumer


Q1: Will project process personal data OR will spec create a link to personal data?
Yes
No
Q2: Will project generate data?
Yes
No
Q3: Will deployment of the project be used in a network device by an individual?
Yes
No
PIA Needed
No PIA Needed
Privacy Findings

# PIA process steps

1. Outline data flow between internal interactors within the product.
2. Outline data flow between the internal interactors within the product and interactions of external interactors through associated format, interface or protocol used by the product.
3. Does the product collect, utilize, store, transfer, manage information that could identify a person? Document the classification of personal data in PIA Report.
4. Does the standard collect, utilize, store, transfer, manage information that could identify a network connected device? Document the classification of personal data in PIA Report.
5. Identify privacy principles and underlying privacy safeguarding requirements applicable to the product.
6. Outline the threats created by these data flows for instances where a privacy control mechanism can be introduced to safeguard data protection. Document these in the PIA Report.
7. Document in the PIA Report specific approaches, beyond the privacy controls in #6, that will enhance privacy such as limits on collection, limits for retention, rules for secure transfer, rules for data processors or 3rd parties dealing with responsible consumer data, rules for limiting identification or obsfuscation.
8. Identify harms that identified threats could cause, probability of occurrence, probable monetary impact to and mitigations to asssure harm prevention.

***FINDINGS are the actionable items resulting from this analysis***

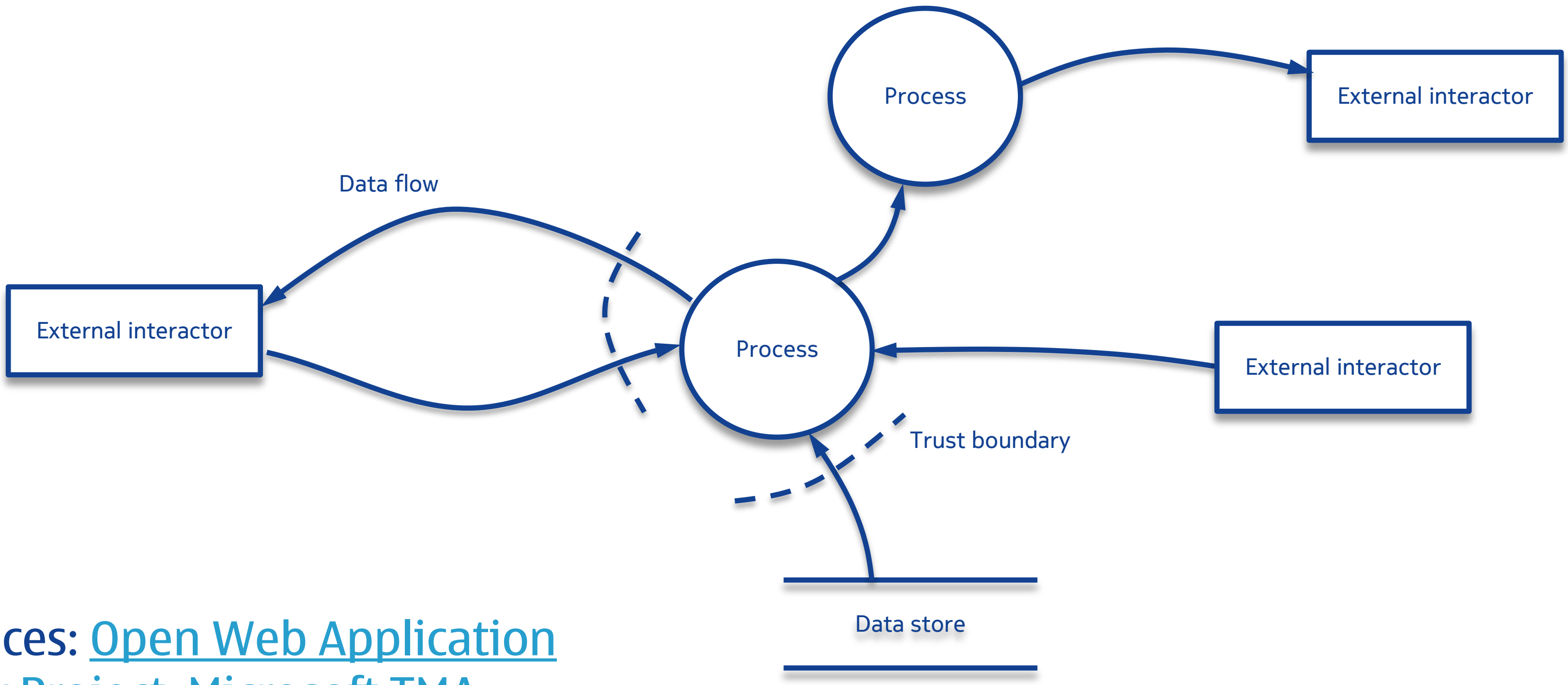
# Data analysis and classification

- Goal of data flow analysis is to be able to identify personal data within the data flows and classify them for privacy impact
- Example categories of personal data might include:
  - Basic data (e.g. first name, last name, mobile number etc.)
  - Address data (e.g. postal code, email address)
  - Restricted categories of data (e.g. racial or ethnic origin, religion, trade union membership – if allowed by applicable law)
  - Social networking related data (e.g. metadata of pictures uploaded, site activity information)
  - Location data (e.g. GPS coordinates or mobile networking positioning information)
  - Identifiers (e.g. IMEI, device identifiers, IP-address)
  - Information on how individual users are accessing the system (log files)
  - Monetary transactions (e.g. credit card number, account information)
  - Other data types (whatever does not fit in any of the other categories)
    - User generated content, Cookies and other tracking tokens, Consents/Prohibitions, Surveys/Questionaires, Confidential communications, Search data
- Classifications of personal data:
  - Not identifiable, Could be identifiable, Identifiable, Sensitive and Identifiable*
- Additional classification questions
  - Description, Collector, Uses, Purpose, Transfers, Disclosures, Storage, Retention, Deletion

*** "PII 2.0", P. Schwartz and D. Solove,**
http://docs.law.gwu.edu/facweb/dsolove/files/BNA-PII-FINAL.pdf

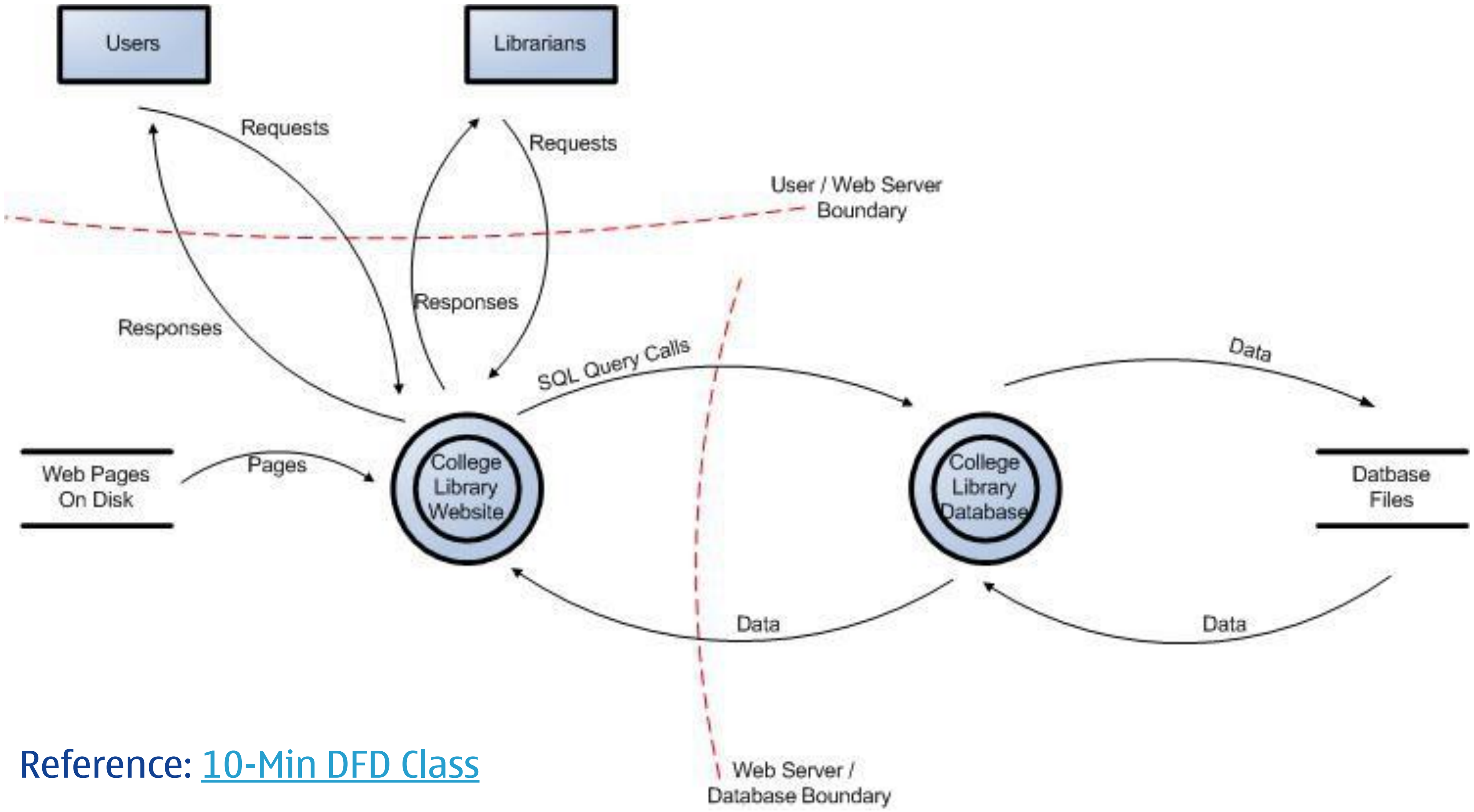
# Threats come with data

- Therefore we model the data using a data flow diagram (DFD)
- Scope is the processes (your code) and all neighbouring actors



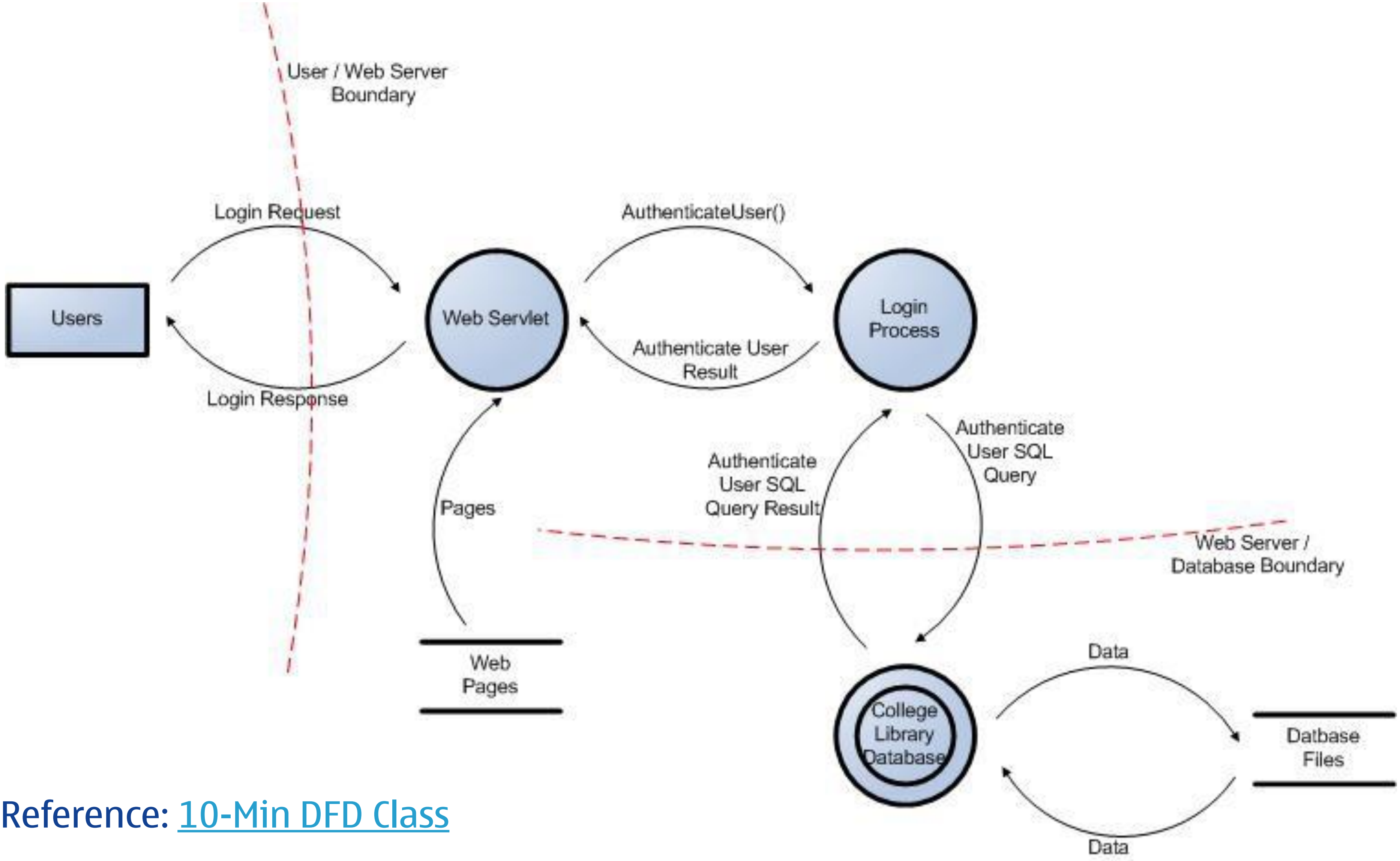
References: Open Web Application Security Project, Microsoft TMA

# Example: College library website



Reference: 10-Min DFD Class

# Example: College library user login



Reference: [10-Min DFD Class]

# What is threat analysis

- Threat analysis is about understanding privacy threats to a system, determining harm from those threats and establishing appropriate migitations (privacy controls or safeguards) against those harms

- Analyzes threats to underlying Privacy Principles at each stage of the Privacy Data Lifecycle

- Analysis results facilitate selection of mitigation Privacy Safeguards/Controls

**Why follow this practice?**

- A structured approach better ensures PbD than an ad hoc approach

- Threat analysis allows development teams to effectively find potential privacy design issues. Mitigation of privacy issues is less expensive when performed during design

- By knowing the threats, privacy testing efforts can be focused more effectively

- This is a prerequisite to conducting a Risk Analysis to mitigate associated harm

# Illustrative table to capture privacy threats

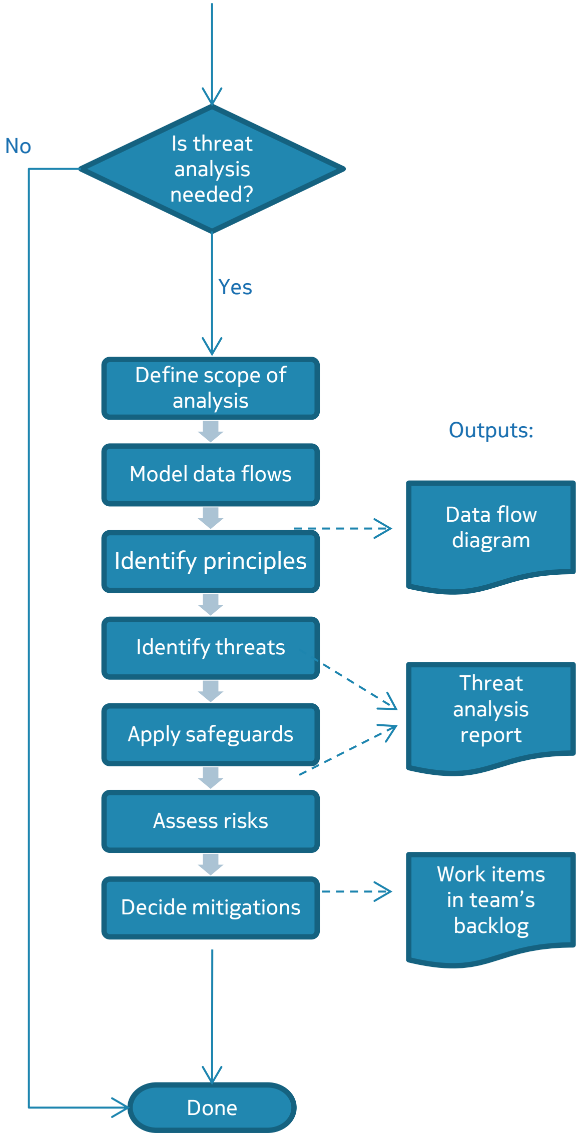
| Lifecycle | Principle | Threat | Controls | Harm |
|---|---|---|---|---|
| Collection | Transparency<br>Notice & Consent | Unauthorized collection | Data analysis<br>Purpose verification | Hidden data bases |
| Collection | Collection limitation | Unlimited collection | Purpose verification<br>Collection method analysis | Lack of proportionality |
| Processing | Purpose specification<br>Legitimate purpose | Processing unrelated to purpose | Function limits<br>User participation | Processing with llegitimate purpose |
| Processing | Processing | Lack of consumer control | Opt-out, Platform privacy control | Automatic processing |
| Processing | Security | Data integrity fault or data misrepresentation | Data integrity check on read, write | Misrepresentation |
| Transfer | Legal obligations | Transfer PII outside EU without consent | Notice & Consent | Violation of EU citizens' basic rights |
| Maintenance | Access & participation, Individual participation, Redress | Lack of consumer redress | Privacy policy includes process for user redress | Inability to rectify errors |

# Threat analysis in PEP

Privacy Engineering Process

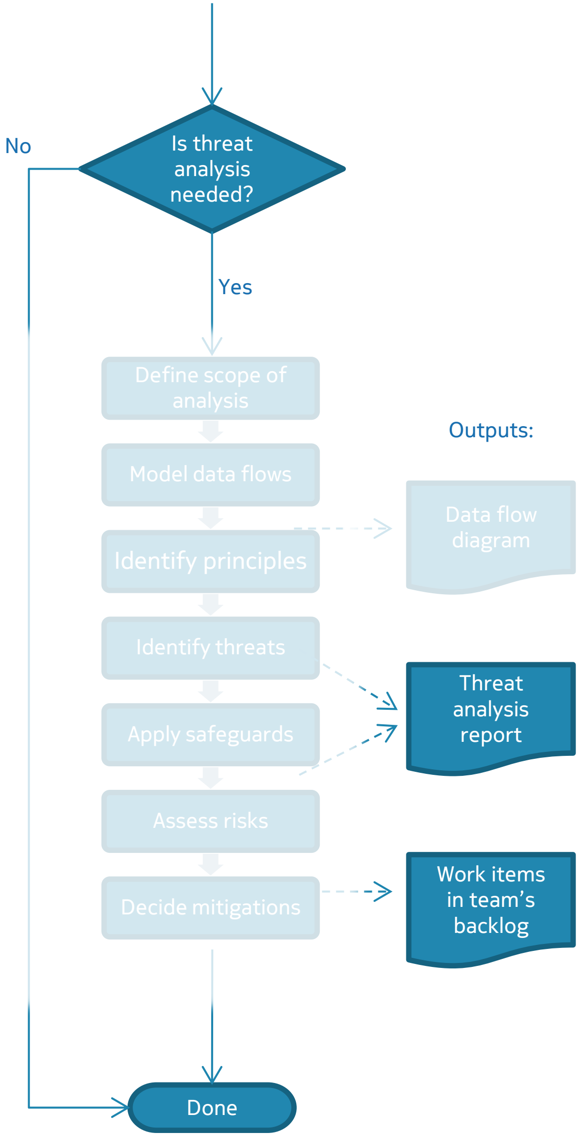
Threat analysis is about

- recognizing associated privacy principles
- understanding privacy threats to a system,
- applying safeguarding controls
- determining risks from those threats and
- establishing appropriate migitations against those risks.



# Privacy review & sign off

- Decisions made in threat analysis are reviewed
  - If threat analysis was skipped, was it justified?
- Completion of planned mitigation actions is verified
- Any remaining risks are signed off by business owner



Was this justified?

Are we ok with decisions and possibly remaining risks?

Are they done and verified?

# Risk analysis

- Objective is to reduce the impact  to the business from the exploitation of a set of threats
- Risk analysis methodologies can be found that are based on business process, information security, project management, etc.
    - ISO 31000, ”Risk Management” standard
    - Information Security Forum (ISF) ”Information Risk Analysis Methodology” (IRAM)
    - Project Management Institute (PMI), Practice Standard for Project Risk Management

- Process utilizes the results of the threat analysis and mitigation activity
- Project business team responsible for completion of risk analysis and mitigation, as knowledge of the business impact is a prerequisite; but technical team provides support

- Risk = Harm * Monetary Value * Probability of Occurrence
- Risk migitation = actionable steps to avoid identified harm

- Migitation approaches include:
    - Do nothing, hope for the best
    - Inform about the risk, with for example a user warning to the risk
    - Mitigate the risk by putting countermeasures in place
    - Accept the risk after evaluating the business impact
    - Transfer the risk with contractual agreements or insurance
    - Terminate the risk, with for example shutdown the data asset

*Security risk is about harm to the company,*
*but privacy risk is about harm to the consumer*

# Privacy design patterns

- Describes a generic solution to a repeating problem
- Format for capturing and sharing design knowledge
- Origins in architecture, O-O Design of software in 90s, to InfoSec in 2000s and more recently to InfoPriv
- Essential elements (POSA format) include:
  - Pattern name, Context, Problem, Solution, Consequences, Known Uses, Related Patterns
- Examples:
  - Informed notice, Explicit consent, Policy update, Visualizing interaction feedback & warnings

✓ ***There is pattern catalog work undeway at http://www.privacypatterns.org***

# Potential evidence of accountability

- Product team management must decide which documents will will form evidence of their accountability, such as:
    - Project description,
    - Data flow diagrams,
    - Data classification (E.G., a Personal Information Inventory),
    - Data management plan,
    - Project specific supplemental privacy policies,
    - Threat analysis and mitigation findings/report,
    - Risk analysis and mitigation findings/report,
    - Action item tracking tickets,
    - Project feature backlogs,
    - Privacy impact assessment report, and
    - Security assessment report.

# Privacy Compared to Security

# Relationship of privacy to security

- **Information Security** (INFOSEC) can be viewed as *control over who may use a computer and information* stored in it
- **Information Privacy** (INFOPRIV) can be viewed as *control over disclosure of computer based information* and who gets access to it
- Therefore, there is a very dependent relationship

*" You can have security without privacy*
*but not privacy without security"*

# Influence of InfoSec on InfoPriv

- Information privacy borrows heavily from InfoSec for organizational governance, concepts, processes and tools
  - Threat analysis and mitigation
  - Risk analysis
  - Control – Vunerability model
  - Implementation frameworks

- InfoPriv differs in a number of key aspects:
  - More elaborate set of guiding principles
  - Goal is for consumer to have control over data
  - Risk Management is about harm to the individual