Privacy by Design with or without Information Security?

Siani Pearson, Cloud and Security Research Lab, HP Labs Europe

January 2013

Privacy by design

…refers to the philosophy and approach of embedding privacy into design specifications….

1. Recognition that privacy interests and concerns must be addressed
2. Application of basic principles expressing universal spheres of privacy protection
3. Early mitigation of privacy concerns when developing information technologies and systems, across the entire information life cycle
4. Need for qualified privacy leadership and/or professional input; and
5. Adoption and integration of privacy-enhancing technologies (PETs)

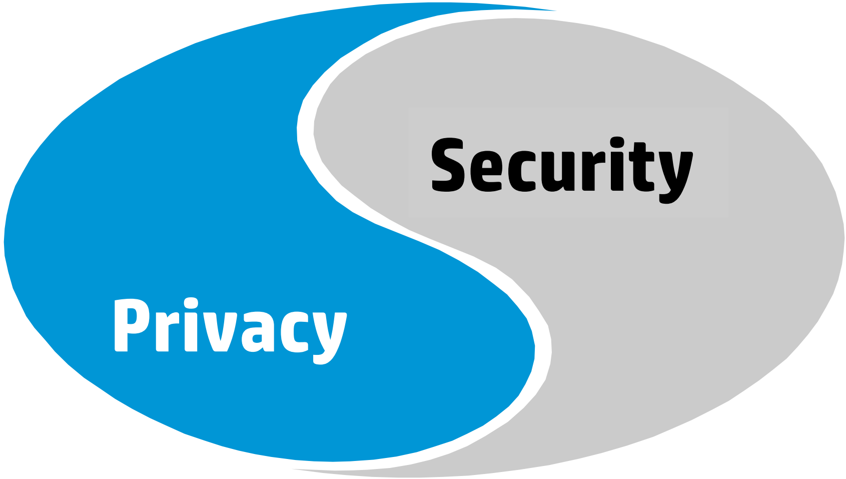
It applies to Products, Services & Business Processes

How are security and privacy different?

Personal Information-Handling Mechanisms

"Individual Rights"

- Fairness of Use
- Notice
- Choice
- Access
- Accountability
- Security



Protection Mechanisms (for any data)

- Authentication
- Access controls
- Availability
- Confidentiality
- Integrity
- Retention
- Storage
- Backup
- Incident response
- Recovery

Many privacy laws also restrict transborder data flow of personal information

Use privacy principles to guide system design

- **Collection limitation**
  – Investigate what data systems are collecting automatically
  – Determine what data you really need and collect only that
- **Data quality**
  – Keep data up to date
  – Use data for relevant purposes
- **Purpose specification**
  – Work out why you are collecting data and explain it in your policy
- **Use limitation**
  – Keep track of purpose for which data was collected; obtain consent for other uses
  – Mechanisms may be needed for obtaining and recording consent
- **Security safeguards**
  – If you collect it, you need to secure it
- **Openness**
  – Users need to be informed of all data collection, including implicit collection – cookies, behavioral tracking, etc.
- **Individual participation**
  – Figure out how you are going to handle access, correction, purging of data
- **Accountability**
  – Be proactive about developing policies, procedures, and software to comply with these principles

Privacy by design

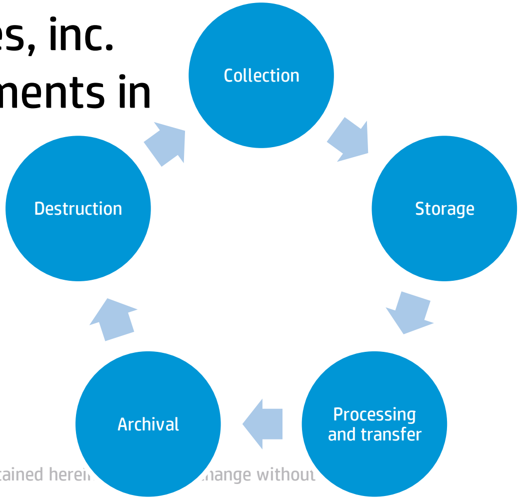
Build privacy into technical solutions by including privacy-enhancing features or through privacy solutions that manage the data from the code level up

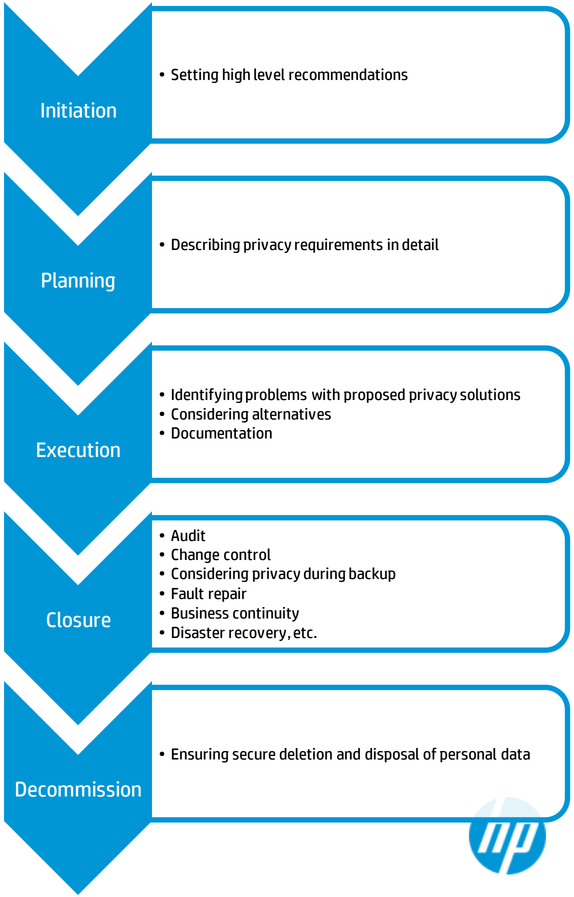
Main Tasks	Security Aspects
Prominent disclosure/notice	Integrity protection of notice; security may be part of the notice
User control	Data access protected via an authentication and authorisation mechanism; integrity of data part of accuracy requirement; security risks should be conveyed to user
Decrease amount of identifiable information collected, stored, tracked and shared	Encryption during transfer and storage, obfuscation, communications inhibitor, secure file deletion may be part of solution; data reduction; data retention

Privacy concerns throughout data lifecycle & design phases

Security aspects within several stages, e.g.

- Secure storage, transfer, retention and disposal (inc. physical security, encryption)
- Disclosure to authorised, authenticated parties
- Data protection plan of third parties, inc. confidentiality and security requirements in vendor management
- Data loss prevention
- Risk assessment
- Compliance and auditing
- Securing backup
- Disaster recovery





Initiation
- Setting high level recommendations

Planning
- Describing privacy requirements in detail

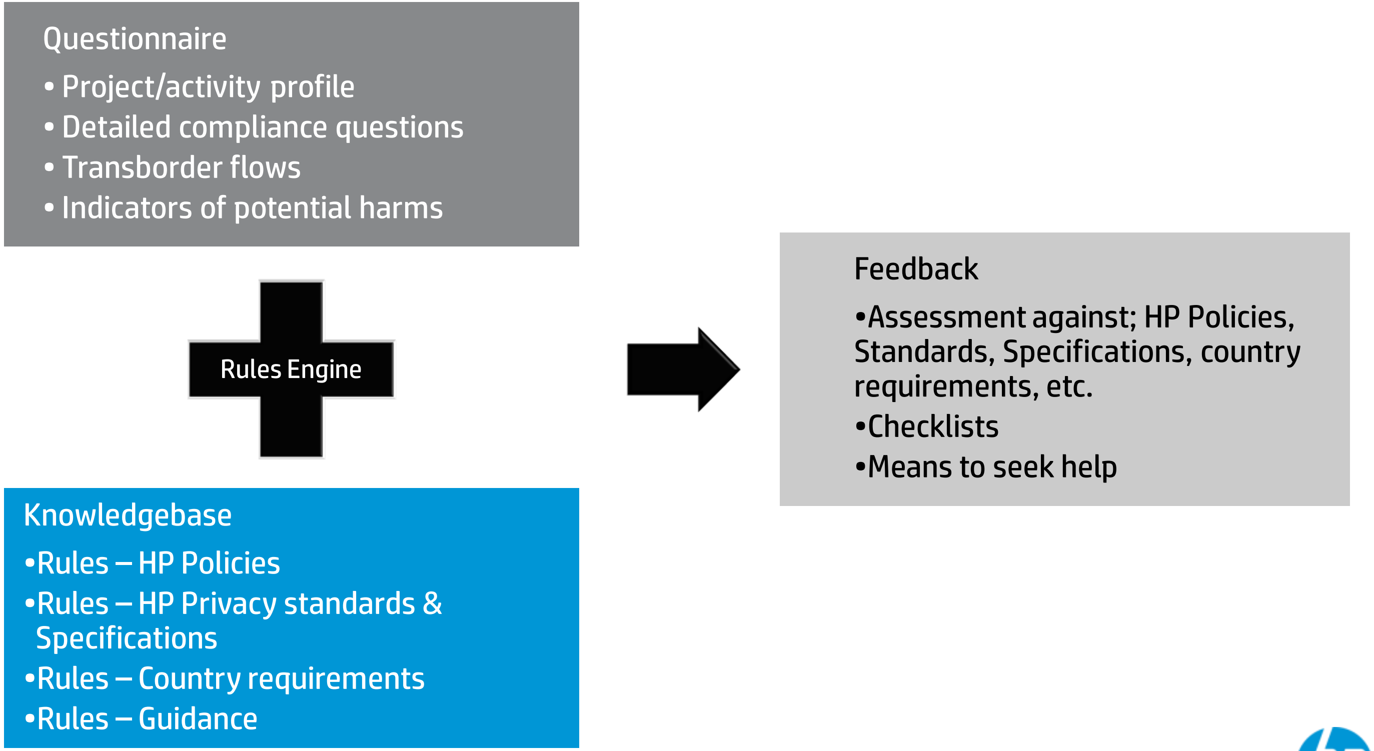
Execution
- Identifying problems with proposed privacy solutions
- Considering alternatives
- Documentation

Closure
- Audit
- Change control
- Considering privacy during backup
- Fault repair
- Business continuity
- Disaster recovery, etc.

Decommission
- Ensuring secure deletion and disposal of personal data

Example 1: HP privacy advisor

Functional Overview



Questionnaire

- Project/activity profile
- Detailed compliance questions
- Transborder flows
- Indicators of potential harms

Rules Engine

Knowledgebase

- Rules – HP Policies
- Rules – HP Privacy standards & Specifications
- Rules – Country requirements
- Rules – Guidance

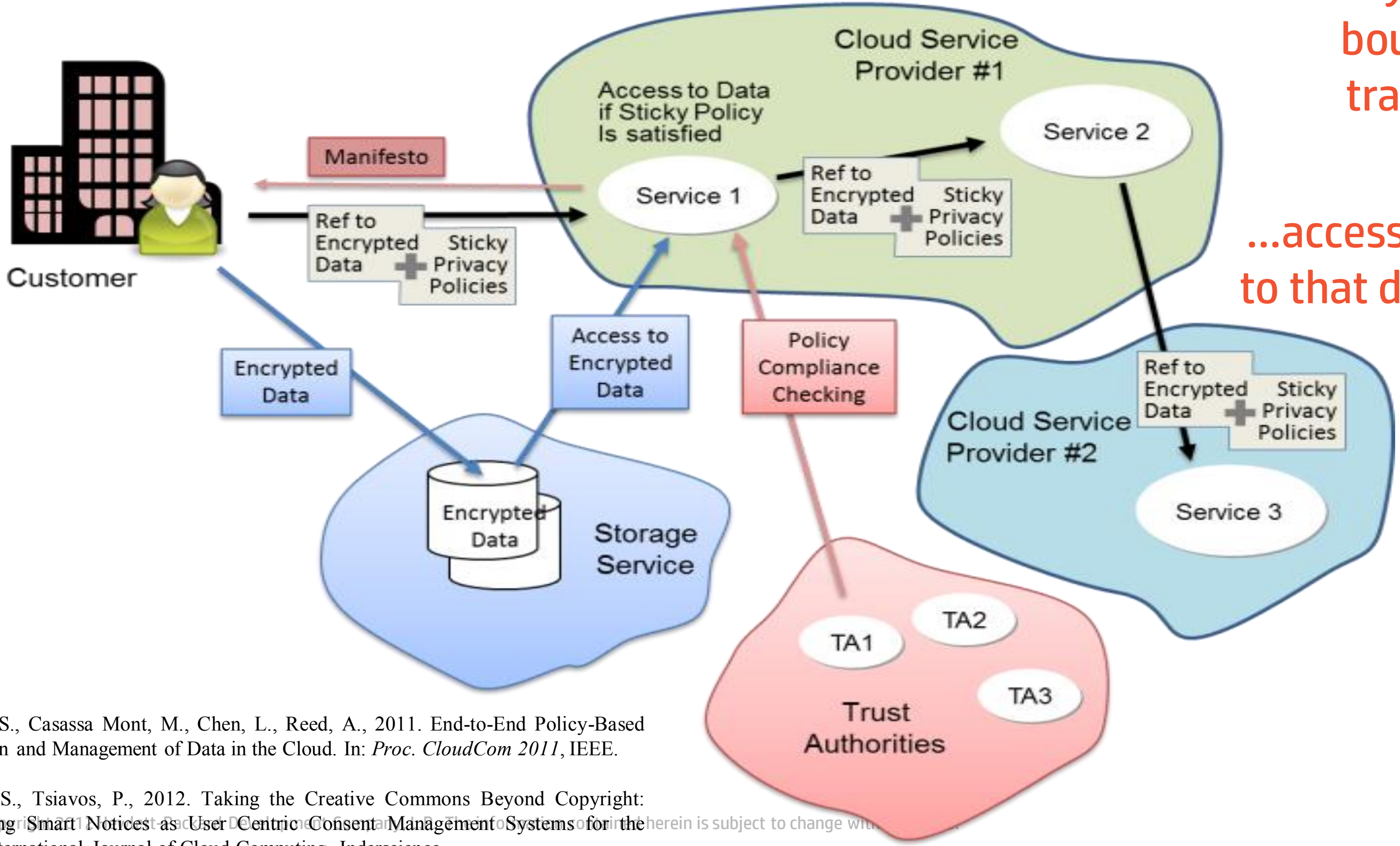
Feedback

- Assessment against; HP Policies, Standards, Specifications, country requirements, etc.
- Checklists
- Means to seek help

Example 2: Sticky policies

Machine readable part of contract generated by smart notice is bound to data as it travels around the cloud…

…access is only allowed to that data if the policy is satisfied



Pearson, S., Casassa Mont, M., Chen, L., Reed, A., 2011. End-to-End Policy-Based Encryption and Management of Data in the Cloud. In: *Proc. CloudCom 2011*, IEEE.

Pearson, S., Tsiavos, P., 2012. Taking the Creative Commons Beyond Copyright: Developing Smart Notices as User Centric Consent Management Systems for the Cloud. International Journal of Cloud Computing, Inderscience.

Privacy by default

Software defaults generally ought to reflect social defaults, legal privacy requirements and what is best for users, not what is best for companies

Privacy by default needs to be considered within privacy by design

- would prohibit the collection, display, or sharing of any personal data without *explicit consent* from the customer.

- not really a security issue, although there are good settings from a privacy point of view related to security aspects, e.g. restricting access to personal data via a *'deny by default' access control policy*

Privacy Enhancing Technologies (PETs)

Can be used to help meet requirements

"… any technology that exists to protect or enhance an individual's privacy" ICO, 2008

Privacy management tools

- Define user-side and enable inspection of service-side policies about handling of personal data, cookie blockers, spam filters, pop up blockers, anti-spyware

Pseudonymisation tools

- e.g. Browsers, email, payment, credentials, voting, MixNets
- Encryption practical for info in transit and storage

How privacy rights are protected

Two different approaches

By policy:

Protection through laws and organizational privacy policies

– Often requires mechanisms to obtain and record consent

– Transparency facilitates choice and accountability

– Technology facilitates compliance and reduces the need to rely solely on trust and external enforcement

– Technology reduces or eliminates manual processing

– Violations still possible due to bad actors, mistakes, government mandates

Notice and choice/consent (opt in/opt out), policy enforcement, transparency, etc.

By architecture:

Protection through technology

– Reduces the need to rely on trust and external enforcement

– Violations only possible if technology fails or the availability of new data or technology defeats protections

– Often viewed as too expensive or restrictive

• Limits the amount of data available for data mining, R&D, targeting, other business purposes

• May require more complicated system architecture, expensive cryptographic operations

Sarah Spiekermann and Lorrie Faith Cranor. Engineering Privacy. IEEE Transactions on Software Engineering. Vo. 35, No. 1, January/February, 2009, pp. 67-82.

http://ssrn.com/abstract=1085333

Technological support possible in many areas…

Technical privacy controls built among federated partners

Risk assessment/privacy impact analysis

Transparency – data tracking mechanisms, automated policy assessment tools, HCI, policy mapping, etc.

Provision of assurance

Giving users control over access to data about themselves

Response to data subject access requests in a timely manner

Formation of machine readable policies reflecting requirements and expectations

Privacy policy enforcement and obligation management

Detection and automated notification of privacy policy violations

Policy-aware transaction logs, monitoring and audit

Authorisation without identification

Role-based access control extended to check data usage purpose

Data minimisation, inc. limiting passive data collection

Attribution, non-repudiation and evidence in case of redress

Anonymisation at different layers…