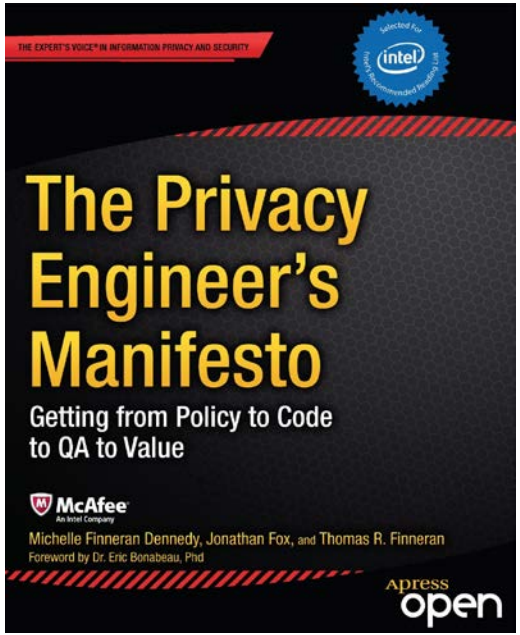
Privacy Engineering for Cloud and Geolocation and Data Governance

Thomas R Finneran

Principal Consultant - IDennedy Project



Some Privacy Requirement Questions related to the Cloud

How does Cloud Provider handle encryption and encrypted data?

Does our user have exclusive access to his or her data?

Does our data get commingled with other people's data? Is the commingling managed effectively?

Can our user access all of his or her data whenever needed?

Does the cloud provider satisfy all compliance requirements including OEDC, FIPPS, GAPP, specific statutory regulations for all jurisdictions, or all enterprise privacy policies?

Is data stored so as to be physically protected?

Can data be transferred without the knowledge of the cloud provider or the data manager/owner?

Are the laws and regulations of all relevant jurisdictions satisfied?

Some Privacy Requirement Questions (Continued)

Can our archiving strategies the enforced within the cloud?

Can we be assured that appropriate data is deleted whereever stored so as not to be subject to a subpoena or a search warrant?

Does the cloud provider manage the data that it stores for its own or someone else's purposes?

Is the cloud provider fully auditable?

Does a cloud provider provide breach notification according to our privacy policies as well as statutory requirements of all jurisdictions affected?

Is the overall cloud provider authentication and authorization sufficient?

Can a cloud provider provide data transfer capability and sufficient security to satisfy data transfer requirements, including to third parties?

Some Privacy Requirement Questions related to the Geolocation Data

Purpose / Necessity:

- Collection and use of geolocation data limited only for the necessary and appropriate use of our systems.
- Ensure that no data use will damage or embarrass a person impacted by our systems.

Openness / Notice:

- Define a Notice Statement explaining to system users how geolocation data will be used, collected, protected, retained, kept accurate, accessed, corrected, and otherwise processed.
- All notice requirements satisfy statutory or regulatory requirements of all jurisdictions.

Choice/Consent:

- Choices concerning geolocation collection and use must be clear and not easily ignored.
- Defaults must be explained clearly and limit not broaden collection and use of geolocation data.

Transfer:

- Geolocation data transferred to and from a third-party must be adequately protected like contract, administrative, technical, logical and physical means.
- Ensure all data transfer complies with laws and regulations of all jurisdictions where transfer is from or to.
- Ensure third parties to whom data is transferred to our vetted from a privacy and security controls perspective.

Some Privacy Requirement Questions related to the Geolocation Data (Cont'd)

Access, Correction, Deletion:

- Ensure that users have a means of accessing personal geolocation information that has been collected about them.
- Ensure that rules concerning correction and deletion are in compliance with laws and regulations of all jurisdictions.

Security:

- Ensure that all system users are authenticated and can only perform functions for which they are authorized.
- Use every technology, statistical methodology, and physical security procedure at our disposal to protect the geolocation data of all data subjects.

Minimization/Proportionality:

- Collect and process only the minimum necessary geolocation data to achieve the identified, legitimate intended purposes.
- Collect and process geolocation data that is proportional to need, purpose, and sensitivity of the information sought.

Retention:

- Retain geolocation data only as long as it is required.
- Ensure that the archiving rules for each date attribute are well-established.
- Consider data destruction tactics such as degaussing or permanently encrypting and destroying keys or overwriting data after the specific deadline.

Data Governance / Stewardship ensures Privacy Requirements are included within our systems

What is Data Governance?

> “Management is the decisions you make. Governance is the structure for making them.” *CIO Magazine* September 2002

Data Governance:

- Is a strategic, “top-down” program in which leadership communicates the core value of data quality and integrity.
- Includes development and enforcement of standards and procedures.
- Requires broad understanding of upstream and downstream stakeholders, systems, and processes for all decisions and issue-resolution.
- Requires executive sponsors to provide support for their business data stewards.

What is Data Stewardship?

> “Data stewardship increases business communications and productivity through business driven and commonly defined data." - Larry English

Data Stewardship

- The willingness to be accountable for a set of business information for the well-being of the larger organization by operating in service of those around us rather than in control.
- Stewardship is not ownership.
  - An owner possesses the rights to something.
  - A steward has accountability for managing something that belongs to someone else.
  - Shareholders who own the tangible assets of the corporation also *own* the information assets. *All* employees, then, are stewards of the information assets.

Stewardship – The key to Data Quality

Data Quality can be maintained by means of:

- **Data Producer Stewards are Business People responsible for:**
  - **Appropriate Data Content Maintenance Quality**
  - **Appropriate Business Rules**
- **Data Usage Stewards are Business People responsible for:**
  - **Appropriate Data Content Use Quality**
  - **Appropriate Business Rules**
  - **Appropriate Presentation**
    - **Vehicle (e.g., Would graphical representation or even video be better?)**
    - **Aesthetics**
- **Data Administration are IT responsible for:**
  - **Data Acquisition**
  - **Data Organizing/Classifying**
  - **Data Storage & Distribution**
  - **Data Archiving**
  - **Data Management (Metadata) Tool Administration**

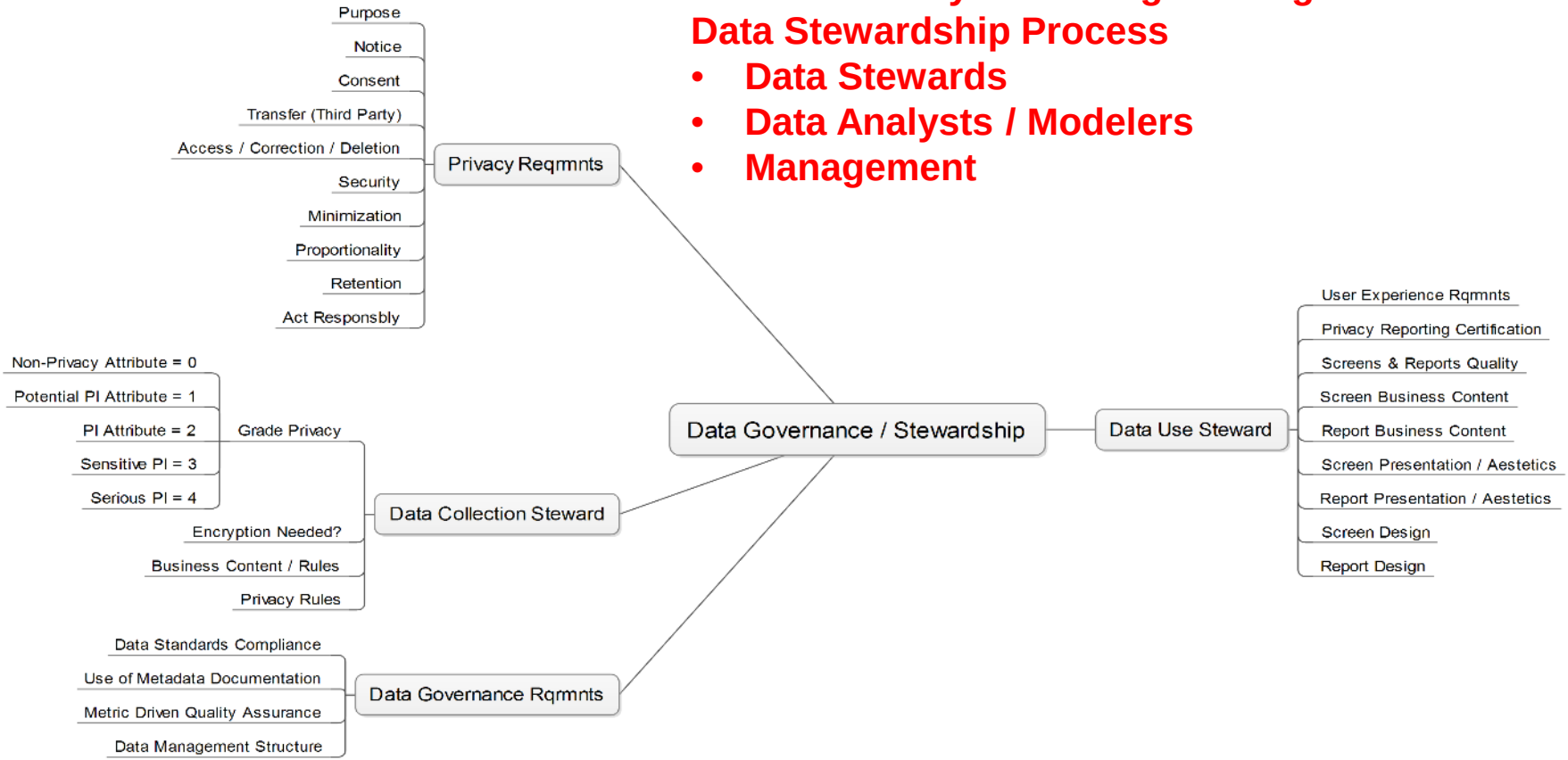
Including Privacy Rules

Including Privacy Rules

Data Governance / Stewardship

Include Privacy Knowledge throughout Data Stewardship Process

- **Data Stewards**
- **Data Analysts / Modelers**
- **Management**



THANK YOU

Questions and More Questions