Privacy Engineering
Bridge to the possible

Michelle Finneran Dennedy @mdennedy
VP and Chief Privacy Officer
December 2018
Data privacy is our future

- Data is essential to digital strategies & innovation
- Technology must meet customer requirements
- As business partners, we must protect our customers’ data & privacy
- New laws & regulations pose huge potential fines & costs; reputational & brand risk
“No matter what market you’re in, no matter what service you provide or product you sell... from right now until the end of time, you’re in the privacy game. Welcome.”

“The Privacy Revolt: The Growing Demand for Privacy-as-a-Service”
*Wired magazine*
How did I get here?
Value of Data

1. Know your data
   - Ownership
   - Inventory
   - Classify

2. Embed controls to protect data
   - Security
   - Privacy
   - Governance

3. Democratize the data
   - Curate to make data accessible
   - Manage processors to policy-based controls

4. Drive business insights
   - Analytics & data science
   - Drive actions

5. MAXIMIZE VALUE
   - Identify AI/ML/product uses
   - Treat data as asset to maximize business intelligence

Enterprise or customer focused

Product or business operation focused
CURATE YOUR DATA
Curate technology

Don’t

Do
Curate retail merchandise

Don’t

Do
Curate digital life

Don’t

Do
“Companies must be good data stewards. If you are not, we will not do business with you.”

US media company in Beacon Group research study, 2018
Path to curation: privacy engineering

- Discipline
- Innovation
- Data-centricity
We are all privacy engineers

A privacy engineer...

• Needs more than just technical skills to **protect** and **extend** the **value** of data
• Draws from artistic **creativity** and expression to **innovate**
• Learns from, **but disregards**, the failures of the past
Privacy engineering: practitioner process
Start with privacy scoping

What market requirements apply?  
What regulations must you meet?  
Whose data are you processing? Where is the data?  
What corporate rules apply?

Gather all document retention periods established by statute or regulation working with...  
Legal team  
Functional teams  
Industry compliance teams  
Records management team  
3rd-party providers
Privacy scoping process

- Scoping
- Develop Class / Data Models
- Develop Requirements Use Cases
- Design Solution
- User Interface Prototype
- Construct Solution
- Quality Assurance
- Roll Out Solution
Scope your environment

Data management, protection and privacy programs, IT & InfoSec

- Where are your employees and customers?
- What applications are you running?
- What data do you use in your processes?
- Where do you process data?
  Collection, use, 3rd-party sharing, analytics

- Whose data are you using?
- Where does data reside?
- Where do your cloud providers securely process data?
- What is your security plan for infrastructure, application, and product development?
Privacy engineering development process
Privacy engineering = setting and executing on privacy requirements

- Data
- Purpose
- Collection means
- Notice
- Choice/consent
- Transfer
- Access, correction, deletion
- Security
- Minimization
- Proportionality
- Retention
- Third parties
- Accountability
Requirements derived from enterprise privacy policy

- 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

Local and international legal, jurisdictional and regulatory necessities
Organization / business requirements
IEEE P7002 Data Privacy Process

- Defines requirements for systems/software engineering process for privacy-oriented considerations regarding products, services, and systems using employee, customer or other external user's personal data.

- Extends across lifecycle from policy through development, quality assurance, and value realization.

- Includes a use case and data model (including metadata).

- Applies to orgs and projects developing and deploying products, systems, processes, and applications that involve personal information.

- With specific procedures, diagrams, and checklists, users perform conformity assessments on their privacy practices.
It’s all connected

Enterprise Architecture

Business Strategy

Technology

Information

Application

Business Results

Application Architecture

User Interface Architecture

Information Architecture
Privacy Requirement Workshops

Five components:
1. Understand context
2. Review use cases and data
3. Understand the user interface and user experience
4. Review context, use cases, data, UI and UX with a privacy filter
5. Review requirements you’ve identified
6. Next steps
Questions help you understand privacy as part of...

System Requirements

Data Requirements

Business Requirements
Based on context and process

If context diagrams and use cases/activity diagrams are not available, we build them in the workshop...
Distill privacy requirements based on...

- **Scope of enterprise**
- **Business drivers**
- **Mission statement**
- **Context diagram**
- **UI and UX design**

- **Action locations**
- **Triggering events**
- **Information flows**
- **Business processes**
- **Other/serendipity**
Context and use case diagrams
Context diagrams

Actors
• Participant Actor
  • Ultimate customer
  • In support of ultimate customer
  • Where located?
• System interface
  • What system?
  • Where located?

Information/control flows
• What information/material/control does user/system supply us?
• What information/material/control do we supply to user/system?

What event triggers the flow?
Use stick figures
Use cases help you gather requirements

- A **use case** is a complete course of events initiated by an actor. **Actors** are people, functional roles, or interfacing systems that interact with the enterprise. Develop one or more use cases for each actor.

- Use cases allow business people to **define requirements in business terms** (business people can write use cases).

- Use cases specify interactions between the actor and business processes, automated or not. Use them to begin to understand system interfaces.
Again, stick figures are fine...
Workshop results

Initial list of privacy requirements (and risks) to consider & solve for during development

It’s a start, not an end
If you can imagine it, you can build the bridge to get you there
For more information

Cisco Trust and Transparency Center

trust.cisco.com

Podcast: www.cisco.com/go/riders

The Privacy Engineer’s Manifesto
free at apress.com

Tweet @mdennedy
The bridge to possible