Operationalizing Privacy in Your Organization

Paola Zeni

EPSC Semi-Annual Coalition – May 10, 2016
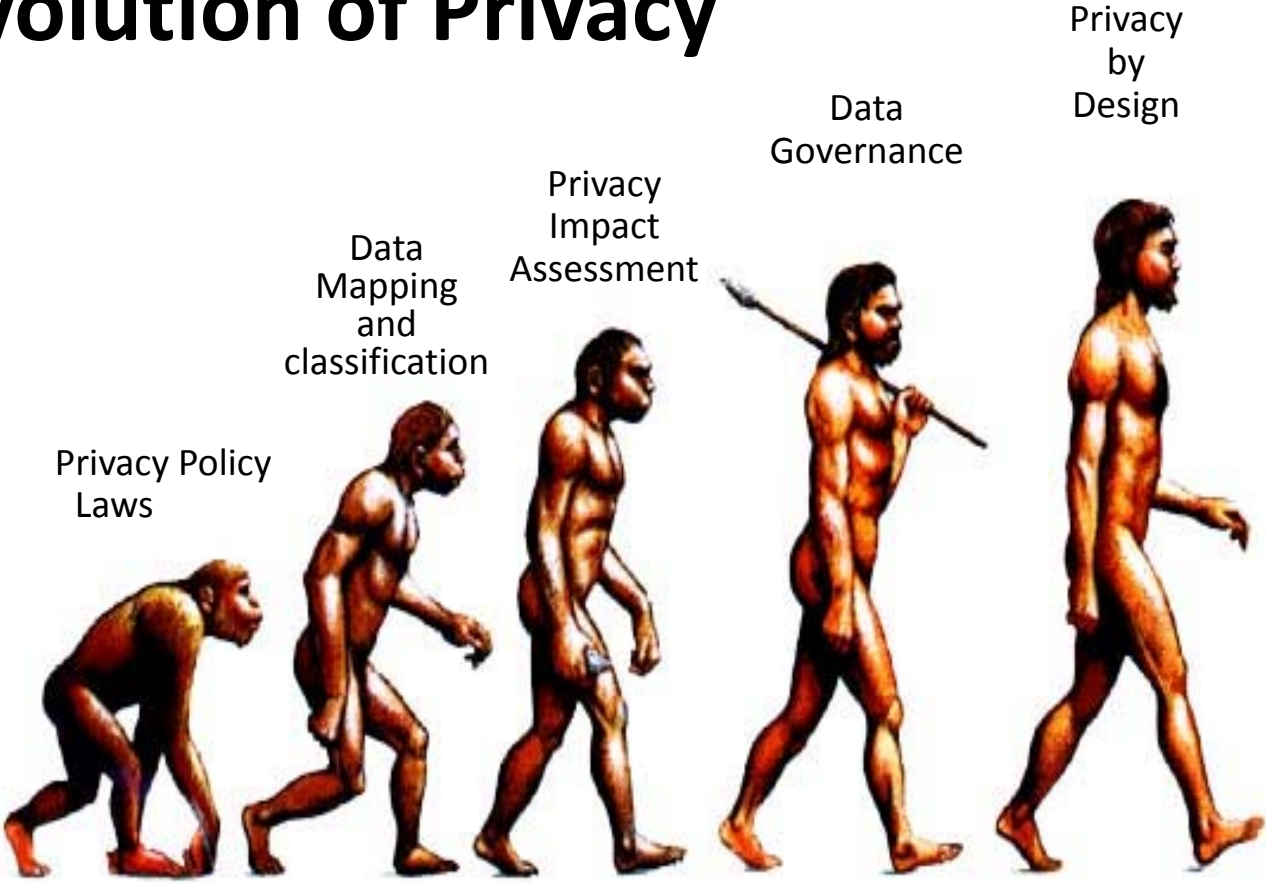
The Global Legal Challenge

US Federal
GLBA, Do Not Call, CAN-SPAM, State Breach Notification Laws, HIPAA, COPPA, FTC Fair Information Practices Safe Harbor Principles

Canada
PIPEDA & Provincial Laws CASL

European Union
EU Data Protection Directive
GDPR 2016
ePrivacy Directive
27 Member States Data Protection Laws
DPA guidelines and decisions

South Korea
Act on Promotion of Information and Communications Network Utilization and Data Protection PIPA

US States
Breach Notification Laws

RUSSIA
Federal Law 152-FZ
Federal Law 242-FZ
Federal Law 526-FZ

PRC
SPAM Regulations

Japan
Data Privacy Act

California
SB1, SB1386, AB 1950

Turkey
Law on Personal Data Protection 2016

Singapore
PDPA 2012

Taiwan
Computer-Processed Personal Data Protection Law

Brazil
Marco Civil da Internet 2014

Hong Kong
Personal Data Privacy Ordinance

Mexico
Ley Federal de Protección de Datos Personales en Posesión de los Particulares 2010

South Africa
Electronic Communications and Transactions Act

India
New rules about reasonable security measures (2011)

Vietnam
Proposed Data Privacy Law

Chile
Law for the Protection of Private Life

Australia
Federal Privacy Act, SPAM Law, State Privacy Regulations

New Zealand
Privacy Act

Argentina
Personal Data Protection Law, Confidentiality of Information Law

Philippines
Data Privacy Law proposed by ITECC

Tools - It's what Humans Build

The Evolution of Privacy

Privacy by Design

Data Governance

Privacy Impact Assessment

Data Mapping and classification

Privacy Policy Laws

The High Level Roadmap

STRATEGY

Connect it to the business

Base your program on principles

Keep it as simple as possible

CHANGE MANAGEMENT

Synch your pace with the organization's

Engage stakeholders

Create a community around privacy

Network, network, network!

RESULTS

Pick your battles

Balance short term wins with long term progress

Standardize

Embed in the organization

Communicate prolifically

Strategy

- Connect it to the business
  - Solve for business criticality
  - Develop your elevator pitch
  - Use the language of your executives
  - Identify risk factors in the business model
  - Don't forget opportunities!

Keep it simple!!

Strategy

- Base your program on principles
  - Map common applicable requirements
  - Adopt the framework that best suits the business
  - Adopt principle-based policies
  - Create a sustainable mechanism to stay abreast of developments

Keep it simple!!

Change Management

- Synch your pace with the organization's
  - Identify the benchmark
  - Work with the CISO and her team
  - Integrate privacy policies with other policies and standards
  - Make sure privacy risks come up in the enterprise risk assessment
  - Leverage ongoing projects
- Engage stakeholders and create a community
  - Identify champions and advocates
  - Make them visible to each other and their organization
  - Provide training
  - Identify obstacles and sceptics
  - Ask for feedback and invite criticism at the right time
- Network, network, network!
  - Communicate prolifically at individual and company level

The Road to Results

- Build a lasting plan
- Pick and choose from privacy, security and auditing best practices

Keep it simple!!

| Scoping | Data Flow Mapping | Gap Assessment/ Risk Ranking | Remediation & Audit | Additional Remediation | Maintenance |

The Process in more Detail

Phases	Scoping	Mapping Data Flows Listing relevant third parties	Review Remediate	Audit	Remediate	
Tasks/Deliverables/Challenges	• Survey tool • Application owners • Asset Inventory	• Data Flow Maps • Third party vendors list	• Project Plans • Timeline			On-going Maintenance
Resources						
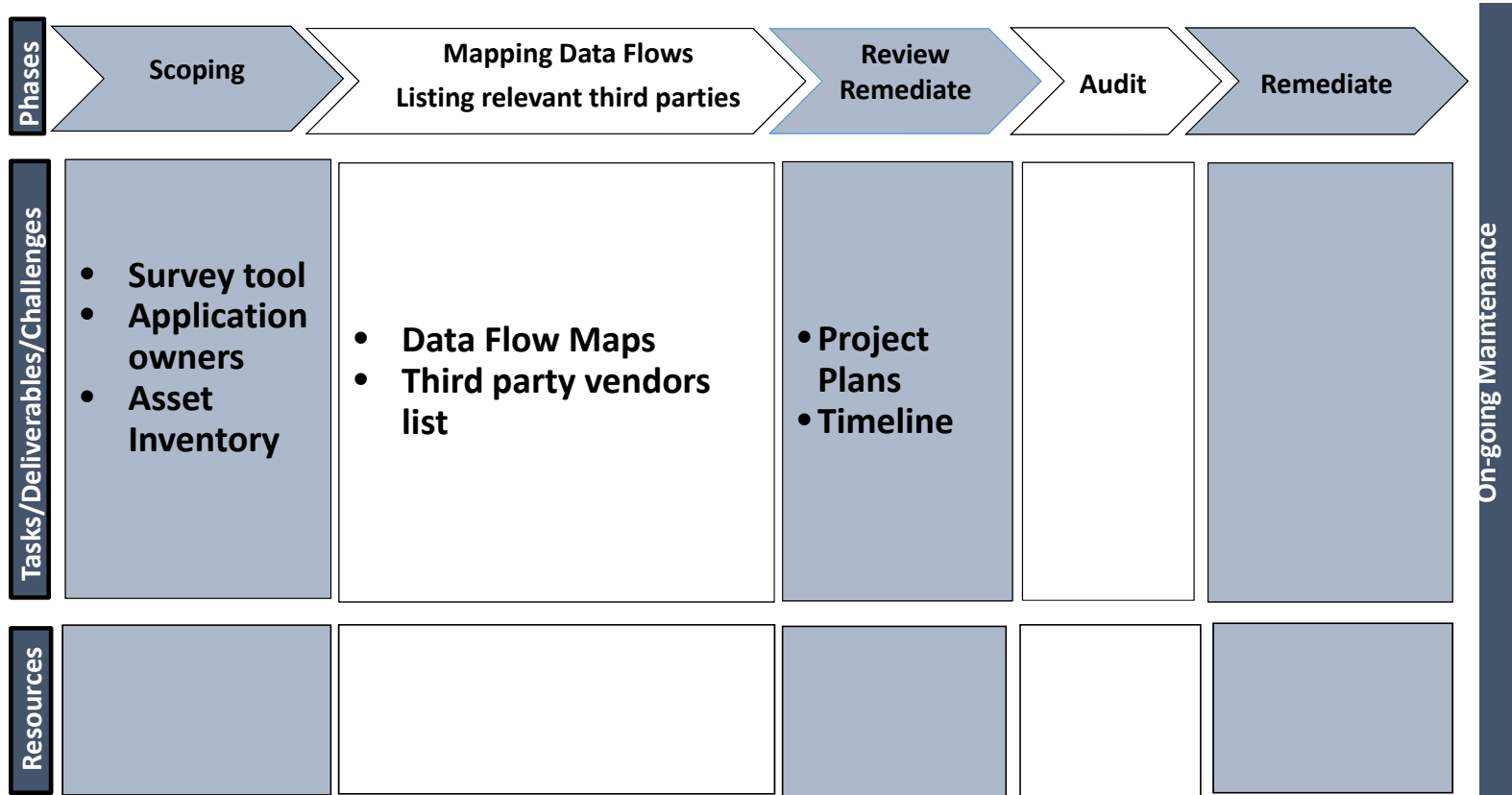
Scoping and Mapping

- **Identify -** Understand the organization
  - What kind of personal data are we processing that is critical to our business?
    - Survey the organization
    - Map business applications that process personal data
    - Identify application owners
    - Do we have data owners?
    - Apply data classification standards
    - Does volume matter?
  - Where is the data located?
    - Jurisdiction
    - Regulatory requirements
  - Can we map the data flows?
    - Identify vendors

Keep it simple!!

Real Time Improvements

- Add Personal Information to data classification standard
- Add Personal Information to the enterprise application repository
- Identify training opportunities and develop training offerings
- Develop a data flow template
- Create a gap assessment questionnaire
- Create your own risk matrix

Assess the Risk

- Survey application owners
- Generate risk score
  - What are the highest risks for personal information?
  - Not all requirements are created equal: apply multipliers to rate risks
- Represent risks to owners and to the organization as a whole
  - Create a heat map

Example Heat Map

Gap Assessment Tips

- Prioritization
  - Leverage scope and mapping
  - Build on the work done by the CISO and by internal audit
- Audit workbook for privacy
  - Create privacy audit toolbox
  - Build privacy audit expertise

Remediation

- Serve it hot!

Thank you!
Any Questions?