Privacy by Design

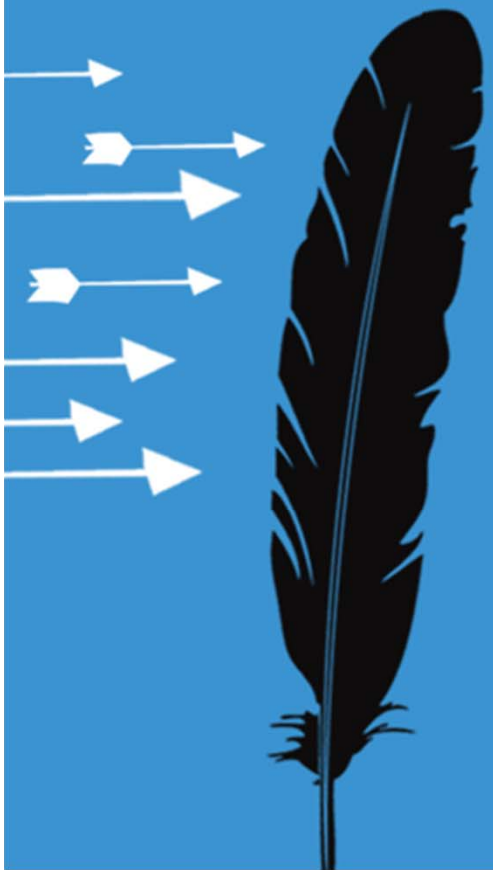
Brendon Lynch, Microsoft
Trevor Hughes, IAPP

Session ID: ASEC-304
Session Classification:

RSA CONFERENCE 2012

Privacy by Design

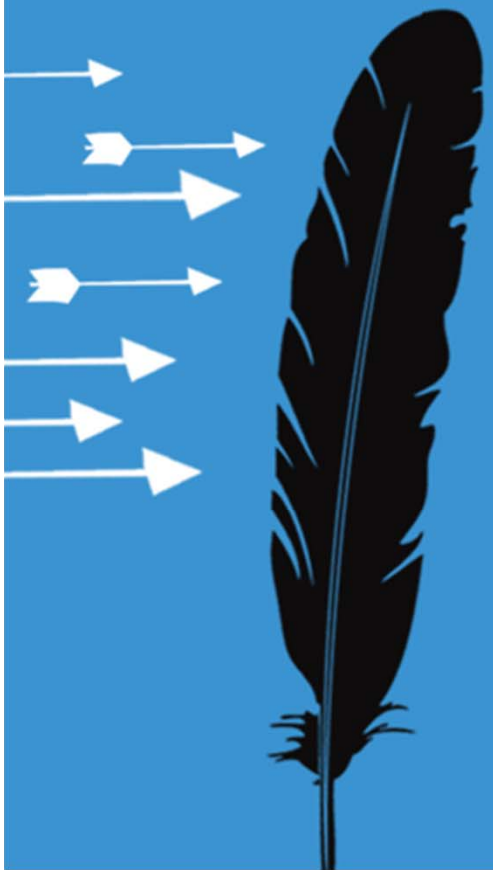
- What is it? Why now?
- Building it. Microsoft Example
- Getting Support.
- Where to Focus.
- Getting Help.
- Education.
- Running, Measuring, and Managing it.



What is Privacy by Design?

Privacy by Design

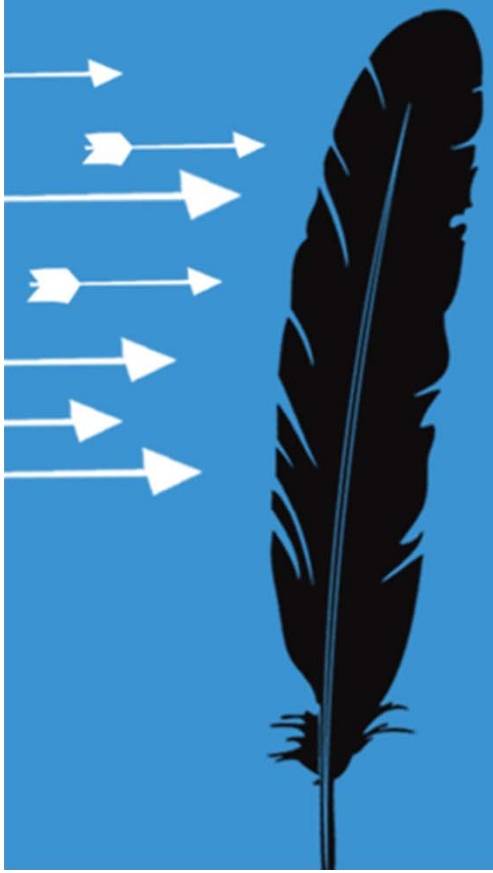
- A broad collection of ideas.
- Championed by Ann Cavoukian, Privacy Commissioner of Ontario
- Basically, build privacy into technology and business processes before launch, not after.



Why now?

Privacy by Design

- As public policy efforts have struggled to respond to privacy concerns, attention has turned to operational solutions
- EU Directive, Framework Review
- FTC
- APEC
- Commerce White Paper



Building it.
Microsoft example.

Trustworthy Computing

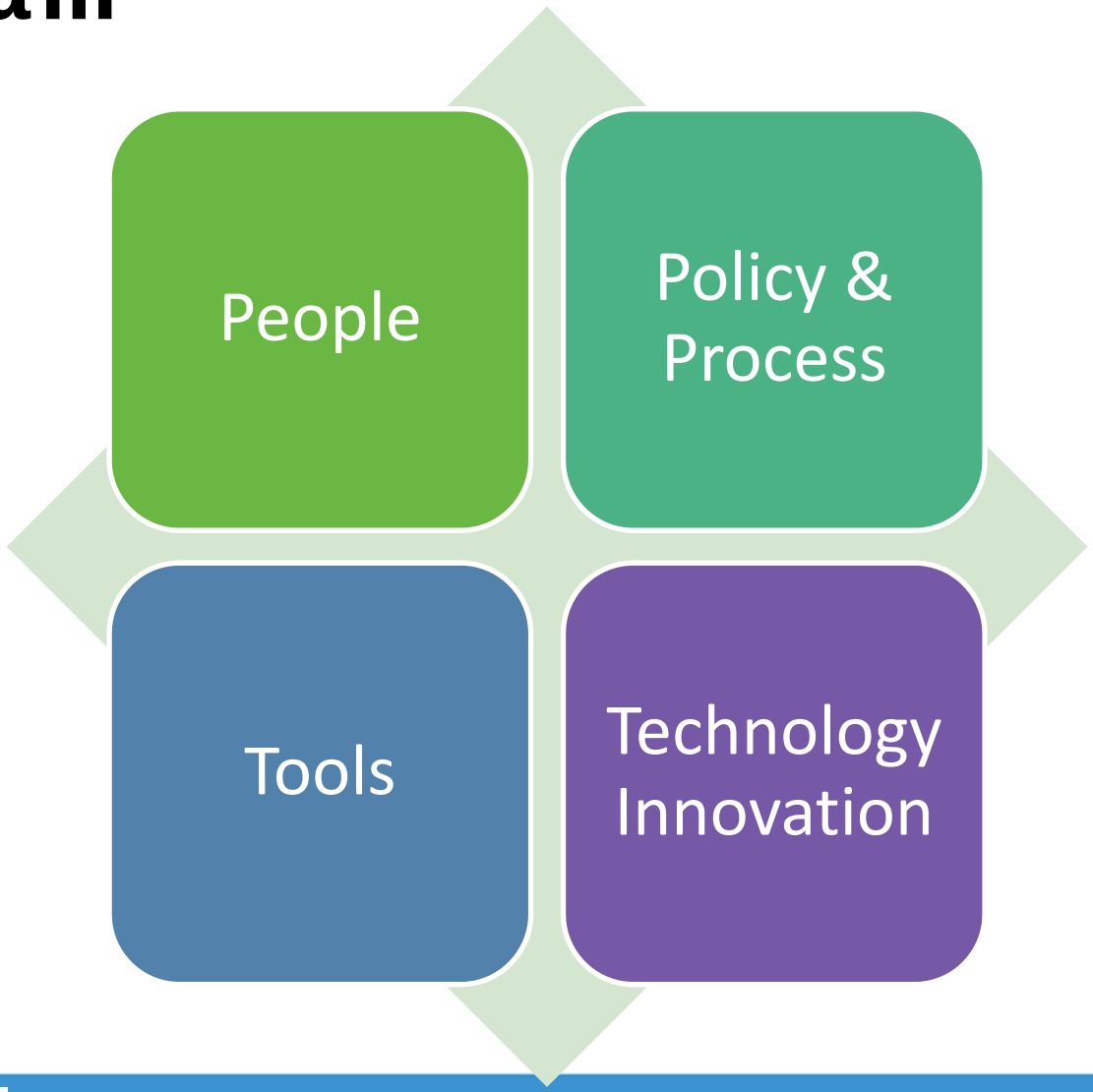
- Secure against attacks
- Protects confidentiality, integrity and availability of data and systems
- Manageable

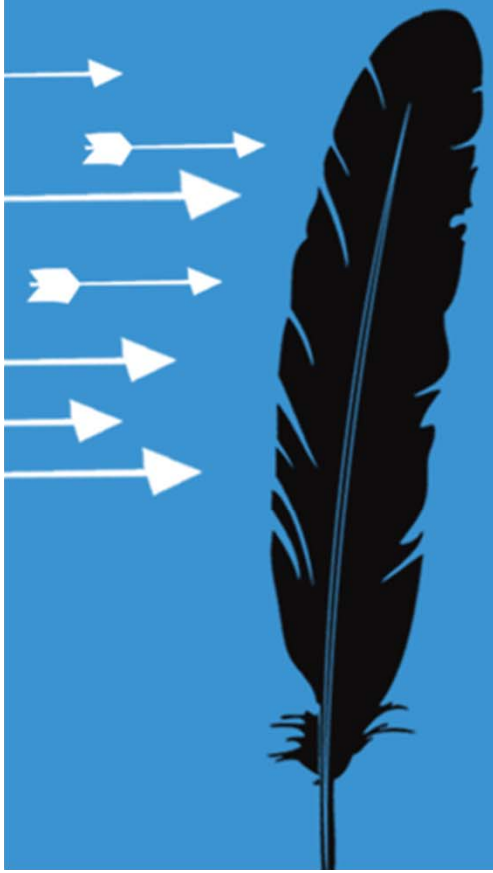
- Protects from unwanted communication
- Controls for informational privacy
- Products, online services adhere to fair information principles

- Dependable, Available
- Predictable, consistent, responsive service
- Maintainable
- Resilient
- Recoverable, easily restored
- Proven, ready

- Commitment to customer-centric interoperability
- Recognized industry leader, world-class partner
- Open, transparent

Microsoft's Privacy Governance Program





People

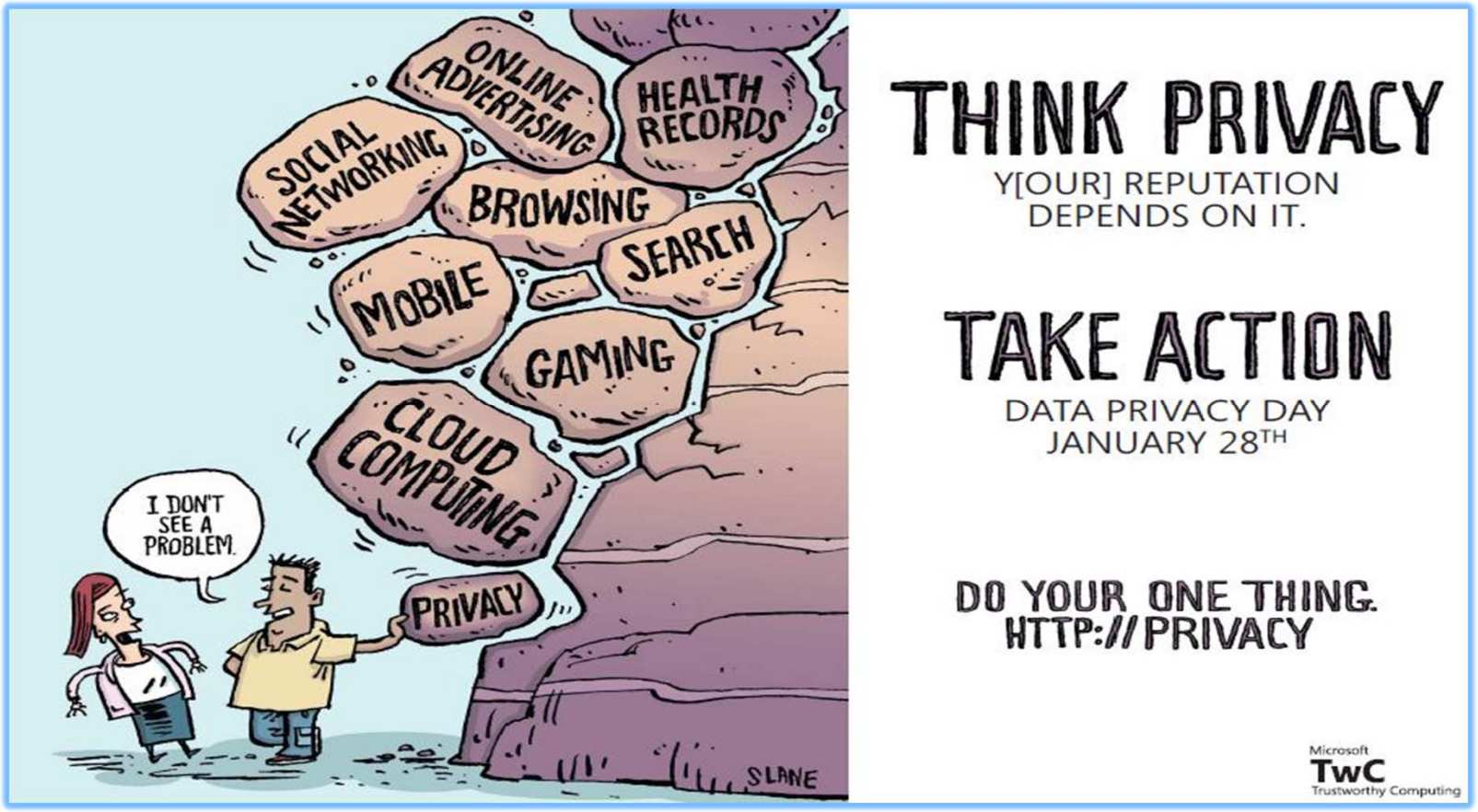
People

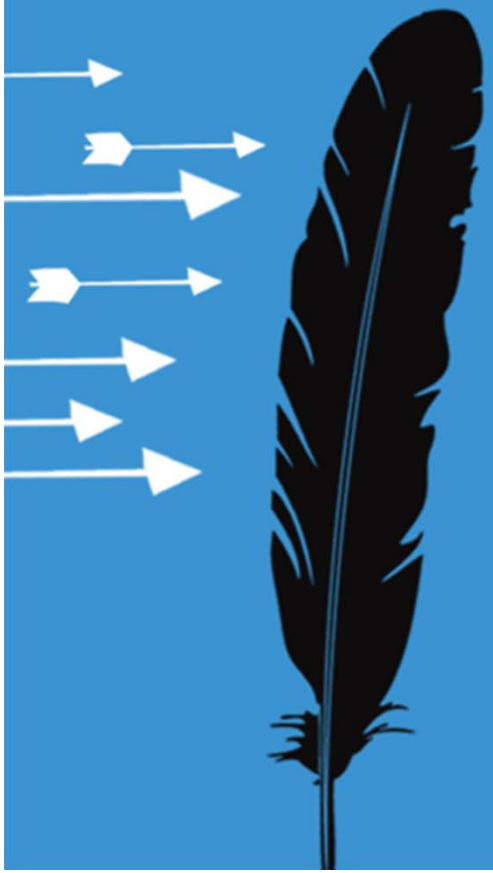
- The Team
  - ~40 full-time privacy professionals
  - ~400 part-time privacy managers and leads
- Expertise
  - Legal
  - Scientists
  - IT Policy and Management
  - Software Engineers
  - Marketing
  - Business


TwC Privacy Team
Legal and Corporate Affairs Privacy Team
Privacy Manager
Privacy Lead
Privacy Champ

Developing Capability

- Onboarding, Mentoring, & Continuing Education





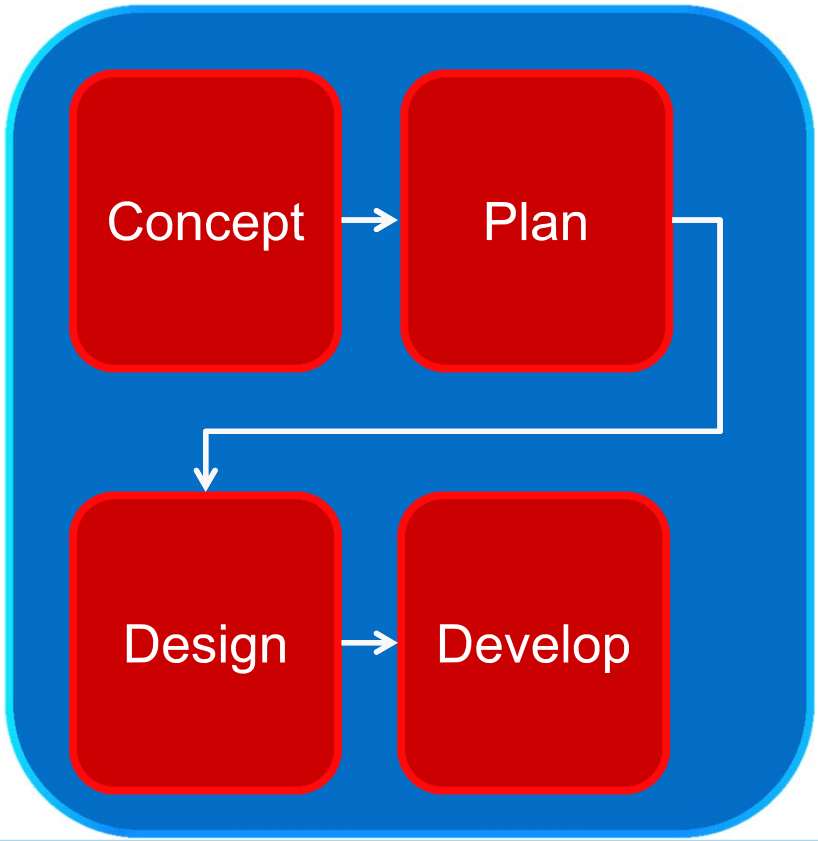
Policy & Process

Microsoft Privacy Standard

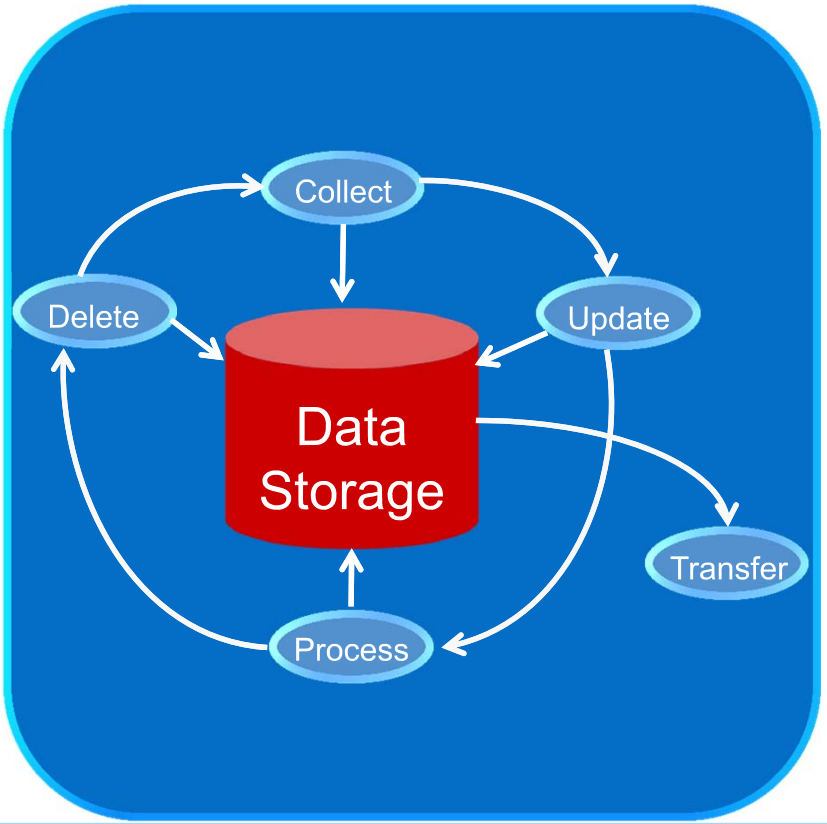
- Software/services development
- Sales and Marketing
- Online Advertising
- Cloud Services
- Location Based Services
- Collection of information from children

Privacy in Products, Services and Other Instances

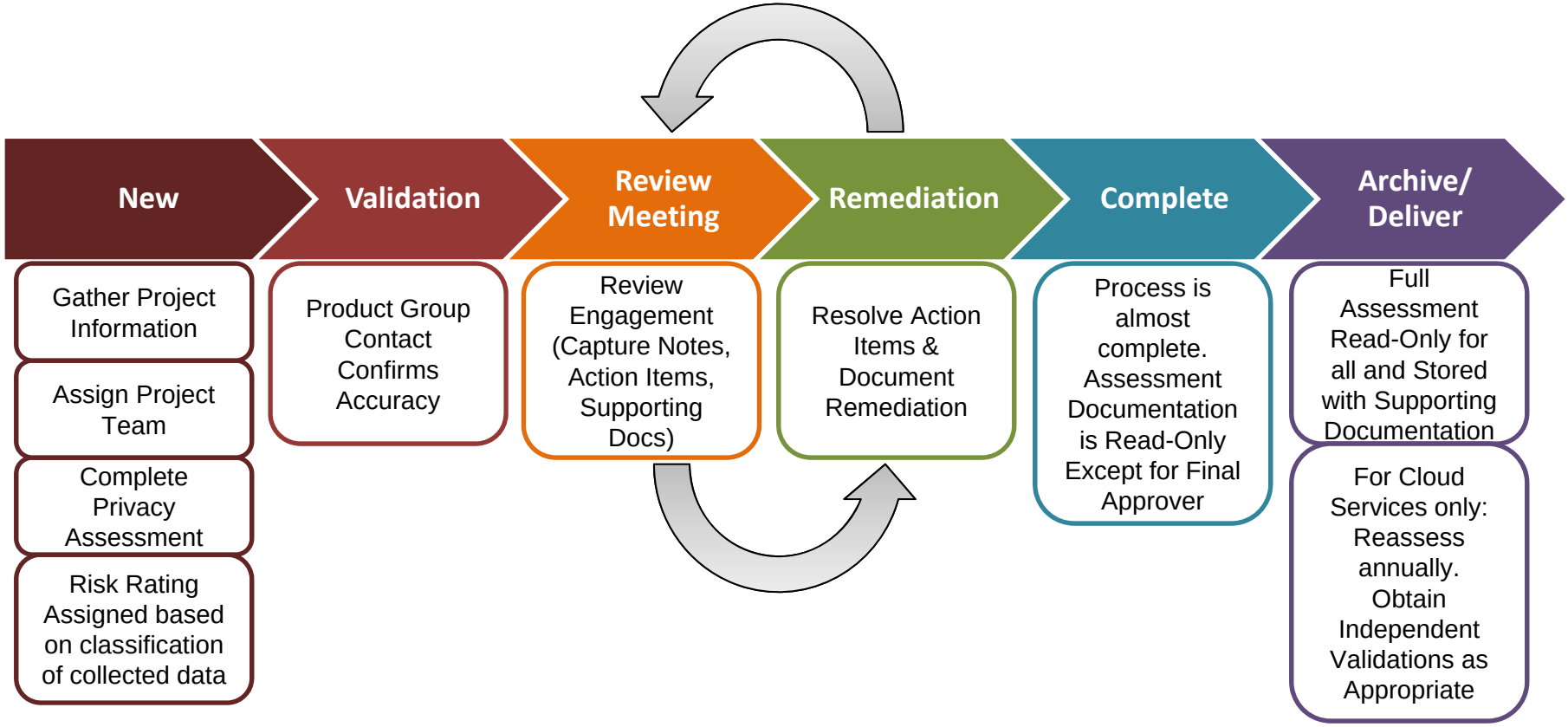
Development Lifecycle



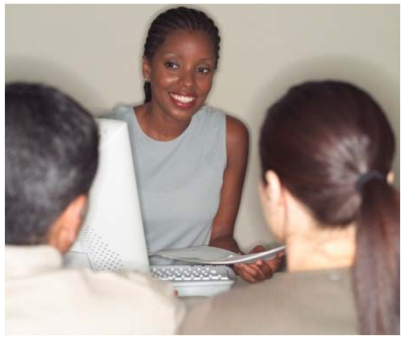
Information Lifecycle



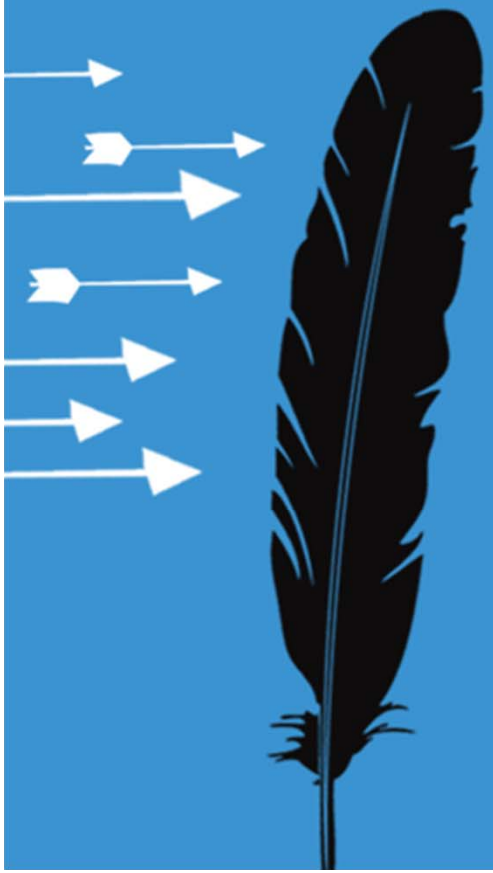
Privacy Review Process



Privacy Reviews

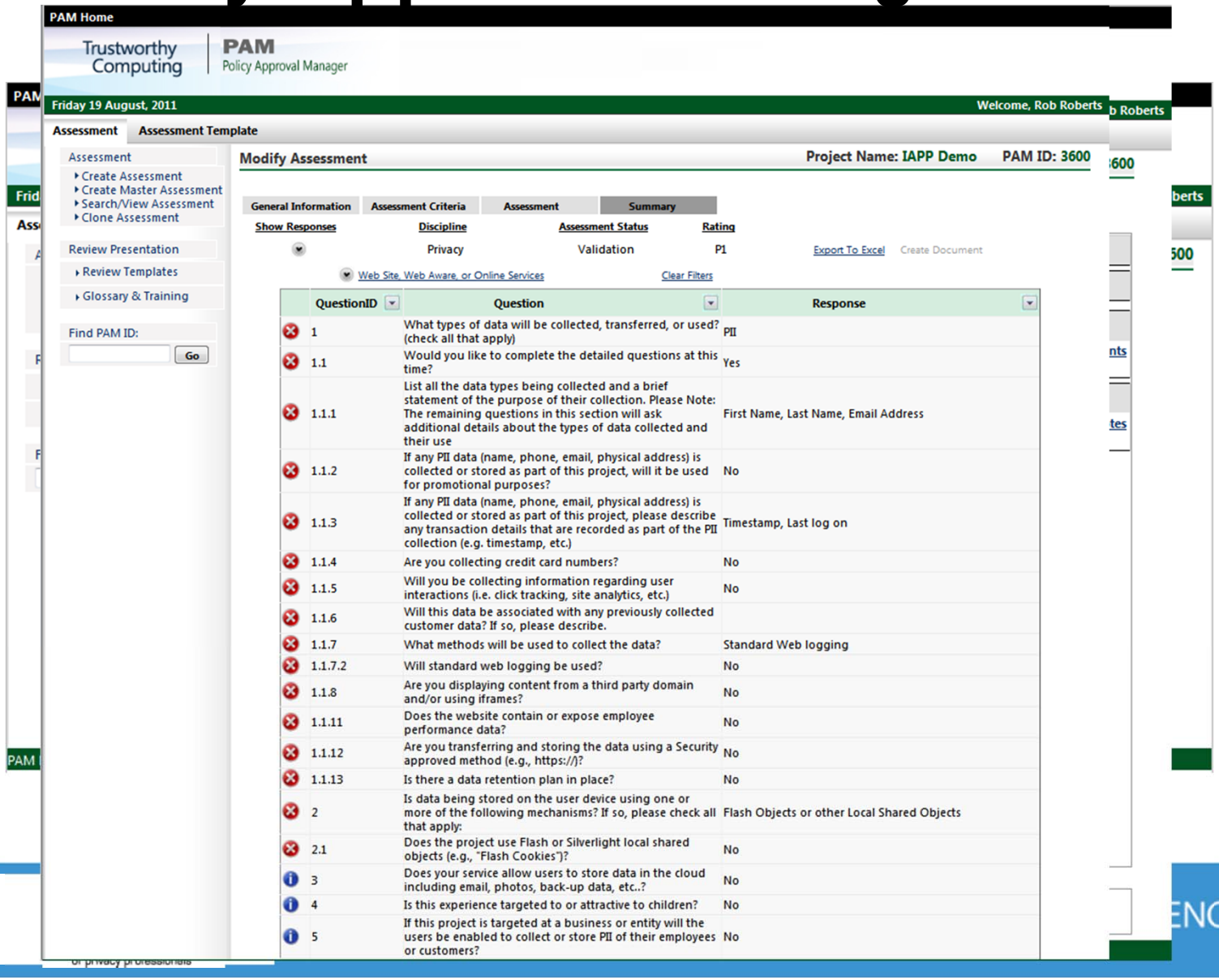


Players	▪ Involve those that can answer questions about the planned project/product/service ▪ Ensure the team understands what they need to provide
Objective	▪ Understand data collection, data use, user experience – ensure compliance with policy/standards
Documentation Requirements	▪ Privacy Approval Manager Complete ▪ User experience screenshots or demo (as applicable) ▪ Marketing materials (websites, emails, etc.) ▪ Previewed by Privacy Champ or Lead

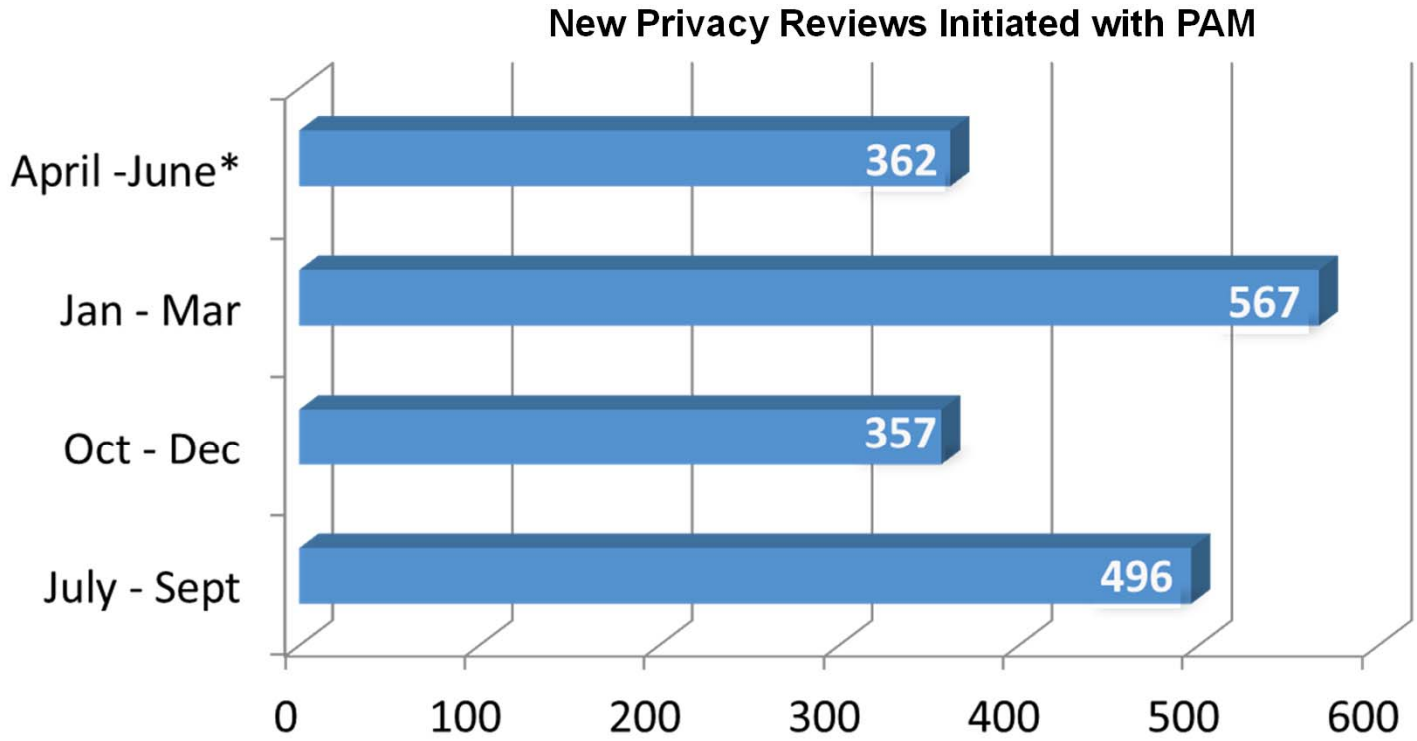


Tools

Policy Approval Manager



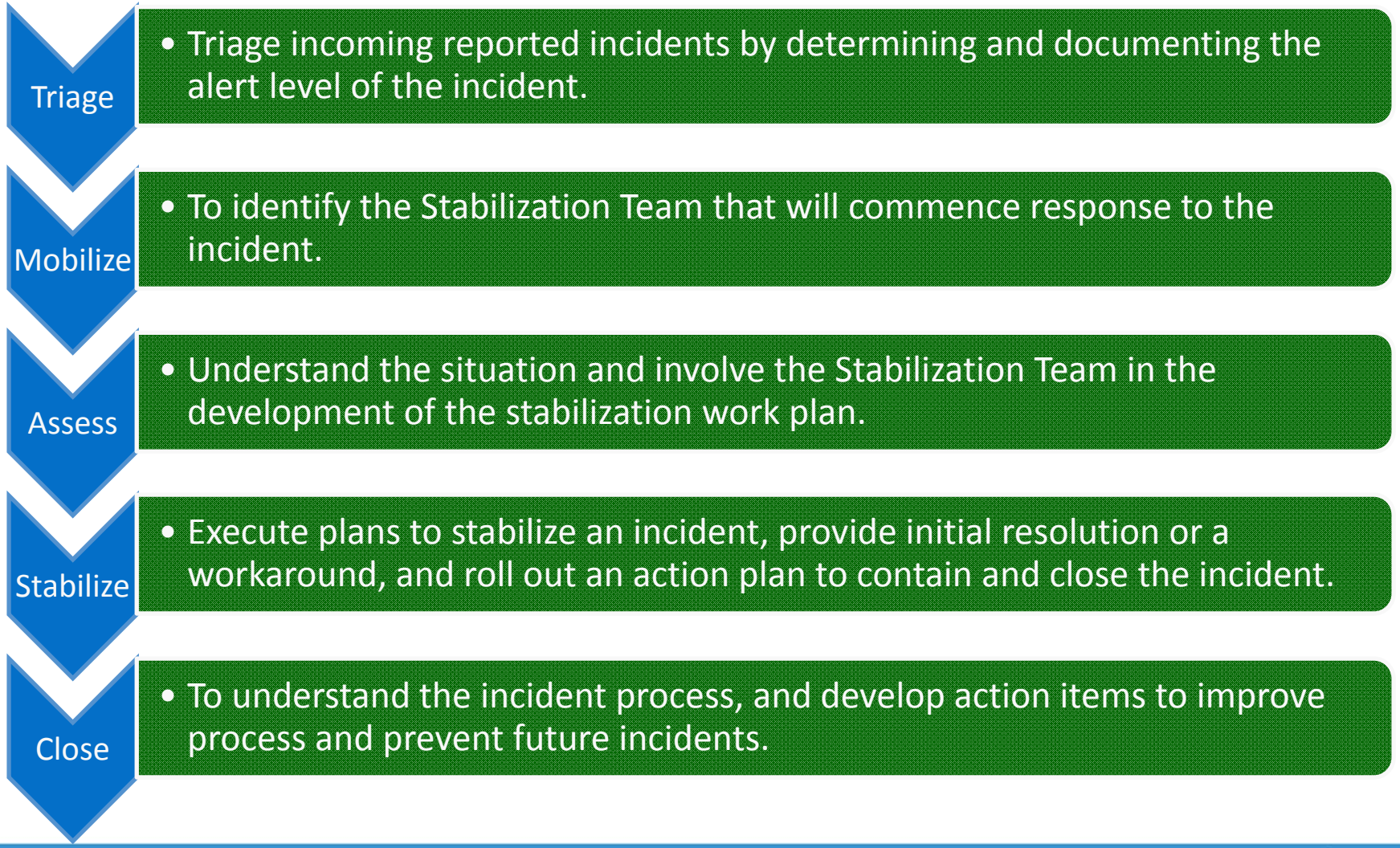
Privacy Risk Mitigation in Practice: The PAM Tool



*Thru June 9, 2011

Since deploying the PAM Tool in July 2010, business groups across Microsoft have used the tool to initiate more than 1,700 privacy reviews

Privacy Escalation Response Process



Case Study: Kinect for Xbox 360

Fast Facts

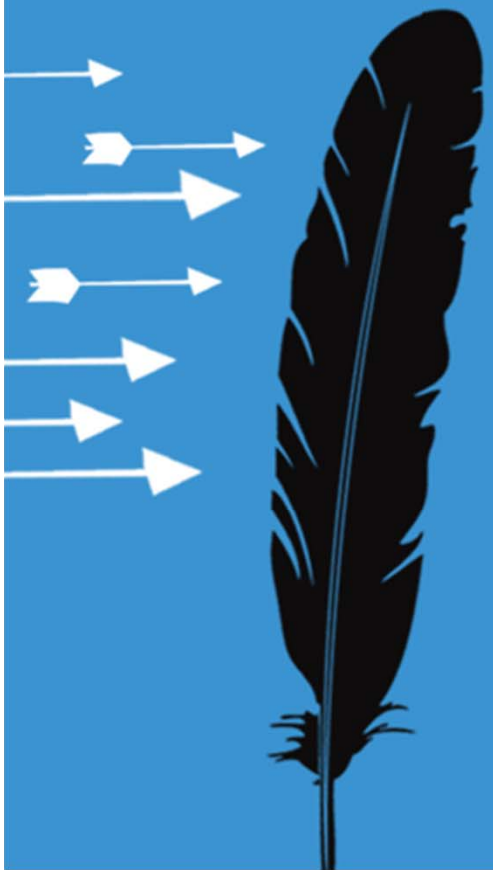
Privacy in Microsoft's Online Gaming Realm Is Serious Business

Case Study: The Privacy Review

Skeletal
- Commands
- Session based, then zapped
- Research use only

Identity
Login using facial recognition

Privacy Solution
Only for service, no promo use
Kept locally on your box



Technology innovation.

Microsoft Research

- Overall, 800+ scientists
  - Computer Science
  - Engineering
  - Psychology
  - Mathematics
  - Physics
  - Sociology
- Privacy projects
  - Database privacy
  - Encryption
  - Social media collective

Privacy Guidelines for Developing Software and Services

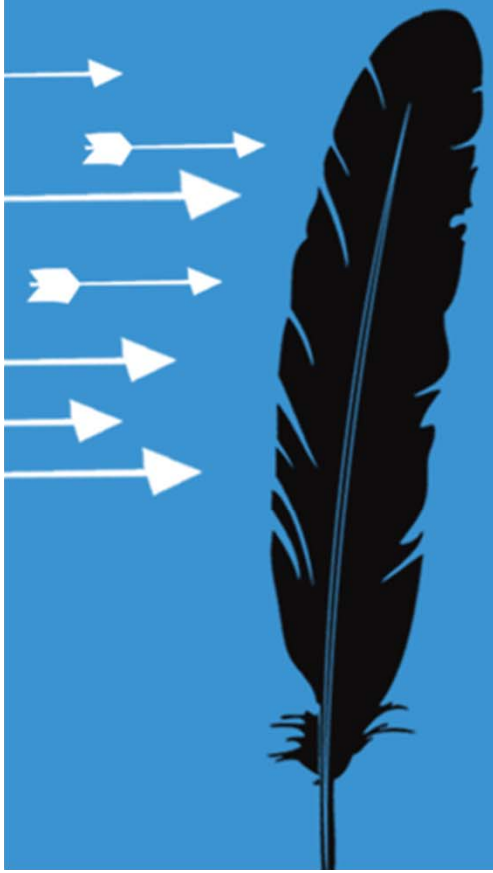
When and how to:

- Provide different types of notice
- Present customers with choices
- Obtain informed consent from users

Data Governance

"How-to" series

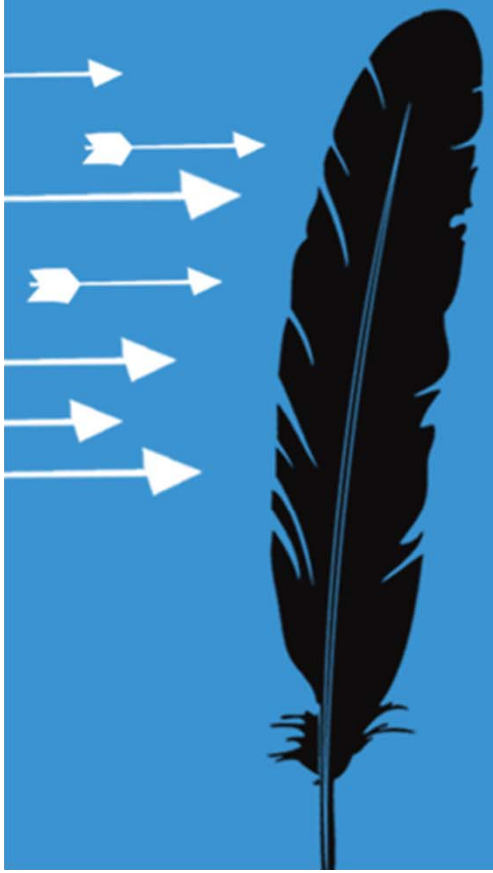
- People
- Process
- Technology
- Cloud Computing



What's Next

What next?

- Privacy by Design is here to stay.
  - Just good business – privacy matters
- Scale according to risk
  - PIAs, governance models, monitoring
  - Management ownership, “skin in the game”
- Watch regulatory developments
  - FTC, Commerce
  - EU framework



Applying Privacy by design.

Applying privacy by design

- Learn more about privacy by design at:
  - http://privacybydesign.ca/
  - http://microsoft.com/privacy/bydesign.aspx
- Implement a comprehensive privacy program covering people, policy, process and tools
- Identify and attach to existing processes where practical (e.g., security assessments)