Privacy Protection in the APEC Framework: The Potential of Technological Tools

Purpose: Information
Submitted by: Oracle
Privacy Protection in the APEC Framework: The Potential of Technological Tools

Joseph Alhadeff
Vice President for Global Public Policy and
Chief Privacy Officer
Oracle
joseph.alhadeff@oracle.com
The Role of Technology
Generally

- Technology is a toil that works in conjunction with, and support of, appropriate policies, practices and procedures
- First develop a privacy policy consistent with the applicable framework, establish the operational practices and determine the procedures.
- Understand the technology tools/functions available
- Optimize for the needs of the organization
Technology In Support Of Multiple Organization Needs

• Too often technology implementations do not support privacy because the “needs” are traded off against each other.

• There is a need to accomplish organization objectives, to secure information and also to protect privacy rights – ALL can be optimized.

• Many of the same functions that enable security and other organization functions also enable privacy.
The Myth of Privacy Enhancing Technologies

- Too often people only focus on those technologies that are designed to support privacy as the only technology tools that support privacy.
- The vast majority of software that is used by an enterprise of any size may be able to support privacy requirements.
- It can only do so, however, if its configured with privacy as one of the objectives.
Privacy Supported in Technology

• Authentication: Who is the end user, who are the users accessing the system on the inside
  – Identity Management
• Authorization: What rights to authenticated users have?
  – Tied to HR system allows for updated management upon change of roles
• Access control: Based on user identity and rights, what content can user access
• Audit: Has user behavior contravened policy
  – Selective audit, fine grain audit, investigatory functions

Encryption: stored and in transit
## Database Technology and the APEC Framework

<table>
<thead>
<tr>
<th>Framework Concept</th>
<th>Tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify Uses of PII</td>
<td>Meta data and permissions</td>
</tr>
<tr>
<td>Choice</td>
<td>Role based access controls</td>
</tr>
<tr>
<td>Integrity</td>
<td>Application based controls</td>
</tr>
<tr>
<td>Security</td>
<td>Recovery to previous state</td>
</tr>
<tr>
<td>Access and Correction</td>
<td>Defense in depth</td>
</tr>
<tr>
<td>Accountability</td>
<td>Label Security, VPD</td>
</tr>
<tr>
<td></td>
<td>Encryption</td>
</tr>
<tr>
<td></td>
<td>Security alerts</td>
</tr>
<tr>
<td></td>
<td>Audit controls</td>
</tr>
</tbody>
</table>

Supporting Today’s Information Flows: Policy and Tech

**Commercial/E-government**
- Privacy Policy
- Privacy Notice
- Internal controls/PIA
- Training
- Accountable sharing
- Compliance and governance
- Complaint handling
- Enforcement

**Implementation**
- Practices and procedures
- Short form
- Technology tools
- E-learning
- Agreements, MOU, Bridge…
- Policies and Rules
- Customer service training
- Internal procedures and cooperation with authorities
Complex Business Transaction

I.M. Buyer
Country A

Compurivacy (CP)
Country B

McVIsAmex

CP Order Processing
Country C

CP Payment Processing
Country D

GeekBags (GB)
Country G

Whine2us
Country I

FedUps
Country F
E-government Citizen Services Hub

- Single source of truth for customer/event definition
- Near real-time data synchronization
- Data cleansing
- Key interactions
- 360 degree view of data with pre-built analytics
- Local control of source info
- Appropriate rule and role-based sharing
- Supports compliance
Centralization and Compliance

Centralization of information may actually increase privacy
• Fault tolerant grid infrastructure
• Single Sign On - Password confusion limited
• Bastion security approach – both moat and security guard models
• Single view of user aids in compliance
• Compliance choke points
  – Privilege management
  – Accountability framework
In Conclusion

- Technology is a facilitating tool, not an end
- You must consider the needs of the organization, including privacy and then optimize the configuration
- Most software has privacy functionality
- Consider the overall information flows and the legal, technology and policy frameworks as well as your overall customer/citizen relationship