The Costs and Benefits of Privacy

Dr. Armgard von Reden,
Chief Privacy Officer IBM Europe, Middle East, Africa

The Costs of Privacy

International Data Protection Conference 2004

1. Cost of Privacy Study

- IBM and Ponemon Institute did the first study of the cost associated with privacy practices of 44 major corporations.
- Results from The 2004 Cost of Privacy Study provide baseline on how large organizations are allocating resources to mitigate privacy risk or to build trust with their key stakeholders.
- Contact Ponemon Institute to obtain copy of the 2004 study.

Privacy Cost Definitions

Key definitions about cost:
- Direct cost – the direct expense outlay to accomplish a given activity (as noted under cost description).
- Indirect cost – the amount of time, effort and other organizational resources spent, but not as direct cash.
- Opportunity cost – cost resulting from inefficient or ineffective compliance, incl cost of failure / non-compliance.

Privacy Cost Activity Centers

Our Study addresses nine core cost centers:
1. Privacy Office – dedicated staff, office overhead, travel and business equipment.
2. Policy & Procedures – creation, review, publication and dissemination of the privacy policy (privacy notice).
3. Downstream Communications – communication and outreach activities.
4. Training & Awareness – education about the privacy policy, program and related concepts.
5. Technologies – privacy technologies, enhance responsible information management, or protect critical infrastructure.
6. Employee Privacy – protection of sensitive employee records, including health care and OSHA claims.
7. Legal Activities – legal review, as well as legal defense costs.
8. Audit & Control – monitoring, verification of privacy program, including self-assessment tools.
9. Redress & Enforcement – investigation and collaboration with law enforcement.

<table>
<thead>
<tr>
<th>Table 1: Privacy Cost by Activity Centers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Direct</td>
</tr>
<tr>
<td>Program Office</td>
</tr>
<tr>
<td>Policy</td>
</tr>
<tr>
<td>Communications</td>
</tr>
<tr>
<td>Training</td>
</tr>
<tr>
<td>Enabling Technology</td>
</tr>
<tr>
<td>Employee Privacy</td>
</tr>
<tr>
<td>Legal</td>
</tr>
<tr>
<td>Audit &amp; Control</td>
</tr>
<tr>
<td>Redress</td>
</tr>
<tr>
<td>Total spending estimates</td>
</tr>
<tr>
<td>Percentage spend by category</td>
</tr>
</tbody>
</table>
II. Costs of legal changes

- The LAW:
- Electronic communication directive opt-in for commercial communication
- Notices statement: opt-in any time revocable
- Transposed slightly differently into national laws

- The Compliance Costs:
- Control of notices statements with help of tool
- Web Crawlers, 5300 pages on the IBM web collect personal data, web crawler for 35 languages of which 28 in the EU
  - For opt-out e-mail management: GECS, 28%
The Future: Information Explosion Continues…
(Actually, it’s accelerating)

**Technology Trends**

- **COMPUTING:**
  - Chips/$: 10x in 5 years
  - Computing power/$: 10x in 4 years

- **STORAGE:**
  - Storage/$: 10x in 6 years

- **COMMUNICATIONS:**
  - Backbone: 100x in 5 years
  - Local loop: 100x in next 5 years

Flexibility and Choice

- Computing as a utility
- Virtualizing the data center
- Server Consolidation
- Usage-based Capacity on demand

Privacy-Enhancing Technologies: Questions

- How to recognize data collectors?
- How to decide which data to provide in a given situation?
- How to keep track of data and identities?
- What can one do with the data received?
- How to enforce correct usage?
- How to enable businesses to work with multiple identities?
- How to authenticate and authorize (de-identified)?
The Future of data privacy:

- Private data becomes a commodity, user decision.
- Privacy becomes much more difficult to control.
- Data transfers become the norm not the exception.
- The access to data is more important than the location.
- The possibilities for misuse increase exponentially.
- The risk for companies and government of misuse increase exponentially as well.
- (Mis)Trust in companies and government will be the issue, data privacy fundamentalists.
- Current level of government and private data privacy protection resources will not be enough to control data privacy in the global economy.

Conclusion: Data Privacy in the future will only exist with the help of PETs

- Technology will enable enterprises and individuals to be more responsive, productive, innovative, resilient.
- Technologies will enable enterprises to be more responsible, compliant, self-controlled.
- Data Privacy Authorities and data privacy officers to work on use of PETs.
- PETs and security technologies are the chance to stay on top of the IT-technology development.

To end on a happy note:

Customers don’t give us their trust, they only lend it to us, if we don’t justify it they take it back.