

Securing Privacy Symposium
Disconnected Privacy: Rethinking the
Organizational Response*
March 13, 2004

*connectedthinking

Outline

- The Organizational View of Privacy
- Divergent Schools of Thought
- Disconnected Privacy
- Strategies for Improving the Organizational Response

Presented by:

Alex Fowler

Co-Director, National Privacy Practice

PricewaterhouseCoopers

E-mail alex.fowler@us.pwc.com

Privacy Landscape: Looking Out



By 2006, 20-30% of Global 1000 will suffer exposure due to privacy mismanagement.

(Gartner, 2003)

- Complex cross-jurisdictional regulatory environment
- Privacy is one of many of laws impacting organizational trust and brand
- Cultural and ethical differences shape concepts of privacy for customers, partners, employees, and competitors
- Rapid technological change
- Intense media pressure on privacy breaches or missteps
- Disproportionate legislative pressure compared with market pressure
- Shareholder pressure is still the strongest external factor

Privacy Landscape: Looking In



By 2006, costs to recover from privacy mistakes will range from \$5 - \$20 million.

(Gartner, 2003)

- Decentralized business structures
- Multiple objectives, operating principles, and incentives
- Varying degrees of professional education, capabilities, and experience
- Rapid technological change
- Uncertainty associated with data handling practices
- Limited resources available for non-revenue-generating activities
- Pressure to achieve cost-savings across the board
- Tendency to focus on security over privacy
- Undefined ROI for privacy
- Complexity in measuring performance associated with privacy

Privacy: Threat or Opportunity?

	Interpretation	Response
<p>Old School</p> <p>“We don't need more laws about privacy. Our operations are already governed by dozens and dozens of laws...”</p>	<ul style="list-style-type: none">• Privacy=Threat• Cost center not growth driver• Shareholder wins	<ul style="list-style-type: none">• Do the minimum to comply with existing laws• Protect status quo (e.g., fight new legislation)
<p>New School</p> <p>“Customers who feel their privacy expectations are met will reward organizations with their loyalty.”</p>	<ul style="list-style-type: none">• Privacy=Opportunity• New way of doing business• Customer wins	<ul style="list-style-type: none">• Permission-based marketing• Brand-oriented• Long-term customer relationships• Embrace change

Old School: Compliance in the Absence of Public Values



HHS

- HIPAA Privacy Rule
- HHS only acts on complaints
- 4000+ complaints filed to date; 100/week



Healthcare Institution

- Organizations spend millions
- Required extensive change management
- Don't field-test notice instrument



Patient

- Patient signs a form
- Patient has to decide whether rights have been violated

What's the point of a compliance effort if it doesn't reduce the chance of an enforcement action?

Old School: Root Causes

Perception=Reality Organization can spend millions on compliance and still not be a trusted brand

Policy Paralysis Organization unable to cope with complex regulatory environment

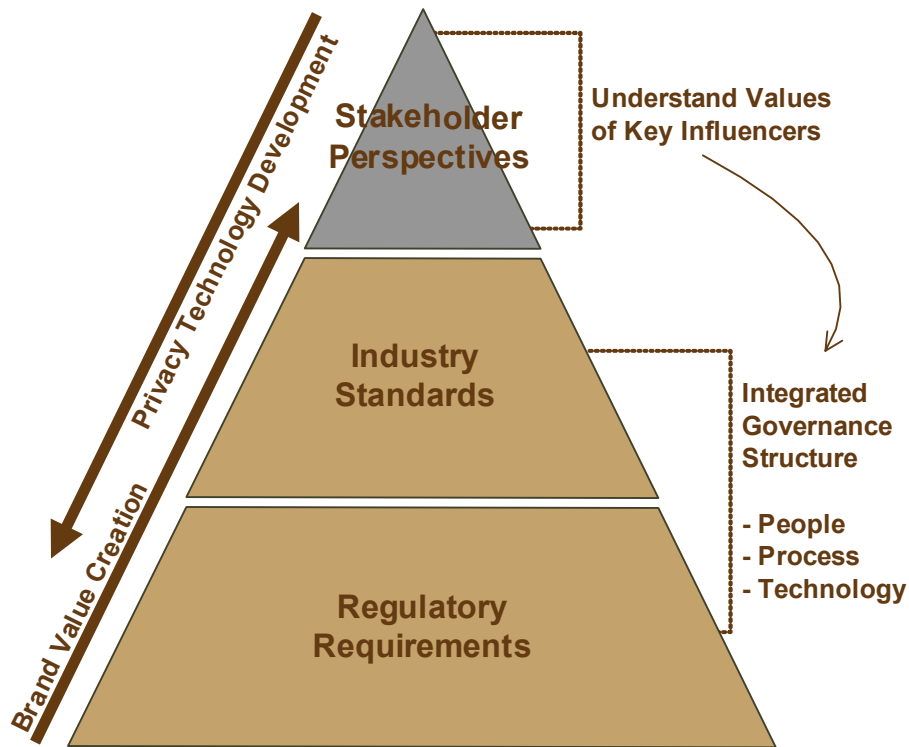
Intentions vs. Incentives Organization rewards data uses in ways that are inconsistent with its intentions for respecting privacy

Data Quantity vs. Data Quality Organization seeks as much customer data as possible, figures out how to commodify it later

Security=Privacy Organization invests heavily in security solutions, mistakenly perceiving it as sufficient for privacy

Online=Offline Organization treats its online customer data activities as unrelated to its offline ones

New School: Develop a Holistic Privacy Framework



- Reduces organizational conflicts arising from privacy
- Allows organization to better determine priorities and allocate resources
- Provides strong foundation in actions that will communicate meaningful compliance activities to stakeholders
- Enables organization to respond to multiple regulations simultaneously vs. sequentially

New School: Issue a Customer Privacy Index



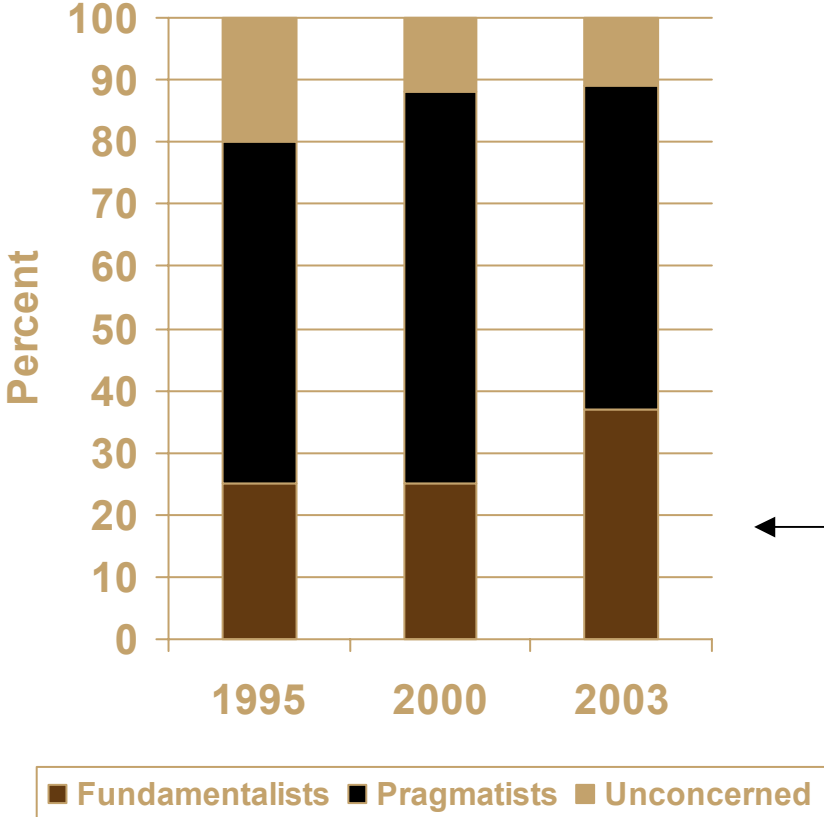
Customer Privacy Index Components

- Qualitative Focus Groups
- Quantitative Survey
- Customer Touchpoint Review
- Privacy Notice Linkage
- Conducted Annually

- Enables a holistic approach by gathering key stakeholder values
- Acts as a filter to better understand and prioritize industry standards and regulatory requirements
- Key strategic input to compliance, including setting policy, controls, and training initiatives

New School: Establish Rapid Response Program

Westin Privacy Segmentation



- “The privacy fundamentalists are the energized segment.” (Westin, 2003)
- Organizations must address fundamentalists

Rapid Response Program

- High-Risk Stakeholder Outreach
- Customer Complaint Resolution
- Incident Response Tracking
- Privacy Notice Linkage

New School: Privacy = Data Management

Trusted Data Handling Program

- Personal Data Map/Flow Diagram
- Data Transfer Strategy
- Centralized Preference Data
- Third-Party Attestations



- Analyze inflows, use, and distribution of sensitive personal data
- Map data handling practices and procedures to existing laws and industry standards
- Develop data transfer strategies, mapping to external/internal rules
- Centralize customer preference data
- Ability to streamline privacy compliance efforts and maximize economies of scale across multiple jurisdictions
- Avoidance of costly system redesign
- Stronger ability to manage privacy controls and audit requirements

Conclusion:

How do we move organizations from the old school to the new school?

Factoring customer values and expectations into the organizational response to privacy needs to go beyond compliance and/or benevolence.