Privacy & Data Protection: Policy & Business Trends

Harriet P. Pearson
VP Regulatory Policy & Chief Privacy Officer

April 26 SIAM Workshop On Practical Privacy-Preserving Data Mining (P3DM’08)
Agenda

- Key drivers of change for business
- Elements of privacy
- Privacy & data protection landscape
- IBM’s global approach
Forces of Change

A new computing model for business

New business models & client needs generated by these new possibilities

The rising tide of globalization
The international era -- exporting
The multinational era -- replicating

20th Century
Today - a globally integrated enterprise...

... *business without borders*
“A ... challenge will be to figure out how to maintain trust in enterprises based on increasingly distributed business models. A company’s standards of governance, transparency, privacy, security and quality need to be maintained even when its products and operations are handled by a dozen organization in as many countries. A reliance on hierarchies contained within one function, enterprise or nation must be supplemented by new ways of establishing trust, based on shared values that cross borders and formal organizations. “

Sam Palmisano, Foreign Affairs (May/June 2006)
Elements of Privacy

Privacy relies on good security
- Many people see them as the same
- Can't achieve privacy without adequate security
- But, can have good security without privacy

Privacy is a shared responsibility
- Government role
- Individual role
- Private sector role
- Different models by country

An issue of behavior, not only technology
- Policies for collection and use of personally identifiable information are key
- Supported by a strong management system

Trust: Sustainable, long-term relationships
- Client trust
- Employee trust
- Consumer trust

Privacy is personal
- Defined by the individual
- Varies by culture
- One size does not fit all
How Is Managing Privacy Different from Security?

Disclosure Controls

- What data did you see/use?
- For what business purpose?
- Did data subject agree?
- Audit: What data was disclosed, to whom, Why, and was it compliant for policy

Access Controls

- Who are you?
- What groups do you belong to?
- Are you allowed to access this resource?
- Audit: Who logged in and when?

Disclosure (Privacy) Controls

Access (Security) Controls
Segmenting Consumers on Privacy

• Two decades of Harris/Westin consumer privacy surveys document continuing segmentation of US public into three groups

• Percentages in each depend on the issue -- financial and health information privacy scores higher than marketing

• When marketing privacy issues the focus:
  Privacy Intense............. 25-30%
  Privacy Pragmatists....... 55-60%
  Privacy Unconcerned..... 10-12%
Privacy & Data Protection: Global Policy Landscape
Policy Frameworks to Enable Privacy

- **Data Protection Principles (OECD, APEC)**
  - Notice, Choice, Access & Accuracy, Security, Fairness, Collection Limitation, Data Minimization
  - Implemented differently by country (e.g. EU, US, Japan)

- **Sector-specific laws (e.g. US HIPAA)**

- **Market self-governance (codes of conduct, online privacy guidelines)**
  - E.g. Behavioral targeting best practices in online advertising
Privacy Regulation around the Globe

European Union

Canada
- PIPEDA (2001 - 2004)

U.S. – Sectoral
- Children's Privacy; COPPA (1999)
- Financial Sector GLB (2001)
- Health Sector; HIPAA (2002)
- California Privacy; (2005)

APEC

Taiwan

South Korea

Russia
- Federal law on Pers Data (January 2007)

Japan
- Personal Data Protection Act (2005)

Australia
- Privacy Amendment Act (2001)

New Zealand
- Privacy Act (1993)

Argentina
- Protection of PD Law (2000)

Chile
- Protection of Private Life Law (1999)

Dubai
- Data Protection Law (January 2007)

Russia
- Federal law on Pers Data (January 2007)

Japan
- Personal Data Protection Act (2005)
EU Data Protection Directive

- Governs transfers of personal information of consumers, businesses and employees
- Variations exist among EU member states
- Member states must create supervisory agencies (data protection authorities) to oversee implementation
EU Data Transfer Options

- EU Data Protection Directive restricts data transfers to non-EU countries that do not provide an “adequate” level of data protection

- Country legislation that provides an adequate level of protection:
  - US safe harbor; Argentina, Canada, Switzerland, Australia

- Options available for data transfers to other countries
  - Consent
  - Safe Harbor
  - Model contracts
  - Binding corporate rules
Other National Laws

- Japan Personal Data Protection Act (PIPA)
- Canada Personal Information Protection and Electronic Documents Act (PIPEDA)
- India – self-regulation in progress
- China – regulation in progress
- Philippines – regulation in progress
Global Accountability Initiative: Cross Border Privacy Rules (CBPRs)

- Alternative model to international data transfer and access under development
- Involvement by APEC, OECD, Canada, Australia, US governments as well as industry
- Main idea: focus on accountability for data handling, rather than specific procedural rules that vary from jurisdiction to jurisdictions and that are ill-suited to modern Internet-enabled data flows
- Global set of principles backed up by private-sector and government accountability mechanism
Privacy & Data Protection: 2008 Environment

- Transparency of data handling practices and incidents
  - Legal requirements to report data incidents de facto present in N America, Australia, UK (public sector), New Zealand, likely to spread
  - Client and regulator expectations for IBM data protection and compliance

- Global integration & personal data flows
  - Continued globalization intensifies regulatory compliance burden related to crossborder data transfers: EU laws are especially complex and pervasive

- Outsourcing & data protection
  - Industry understanding of reasonable practices and risk allocations slowly maturing

- Technology-related issues continue to be active
  - Implications of cloud computing model; identity management; RFID/sensors; social networking; online behavioral tracking; 3D Internet; digital security solutions

- Health care privacy
  - Industry transformation creates opportunities to address privacy via public policy and industry practices, for differentiation as well as compliance/risk management purposes

- National legal models changing:
  - India, EU, US, Australia, Mexico

- National security measures: privacy concerns may affect business operations and create opportunities for new methods
Web 2.0: New Issues & Considerations

- **Role of the individual**
  - As publisher and editor
  - What is the responsibility of the individual to respect privacy (and business confidentiality)?
  - How to support accountability without degrading trust in the workplace?

- **Work-Life Integration**
  - Blurring line between professional and personal
  - Business have always had policies on this, but it now FEELS different.

- **Exposes Fault Lines in Current Policy Models**
  - How do traditional data protection laws keep up with Web 2.0-enabled interactions and knowledge sharing?

- **Need for more-pervasive education/awareness**
  - Privacy protocols, common etiquette/expectations need to be developed and made pervasive
Operationalizing Privacy @ IBM: Case Study
Privacy & Data Protection: Key Organizational Concerns

- How do I organize for privacy?
- What kind of skills do I put in place?
- How does my privacy program relate to security efforts?
- How to define “personal information” and related terms
- Where is the data?
- How do I internationalize or globalize processes?
- What kinds of arrangements do I make with vendors and business partners who access employee or customer data?
- How can technology/automation increase efficiencies or enable data protection?
- How do I respond in the event of a breach?
A Long History…

• Decades of experience
• Innovation in corporate policies
• Industry leadership
• Public policy influence
• CPO leadership
• Privacy Research Institute

“If you want to employ intelligent, sensitive, sophisticated people, privacy is an issue you would better think about.”

Frank T. Cary, Former CEO, IBM
Wall Street Journal (Oct 2, 1975)
A Simple but Aspirational Strategy

- Set the bar for how globally integrated enterprises comply with and manage privacy requirements and issues

- Deliver client value while managing risk

- Engage externally to help shape policy and legal environment
How do we manage privacy at IBM?

- Corporate Guidelines / Policies
- Business Process Governance Model
- Best Practices
- Education/Communication
- Business Controls
- Data Incident Response Process

This is a Closed Loop Process
Online Privacy Education for all IBMers

Welcome to 'Privacy - What you Need to Know'. This course explains IBM’s approach to data privacy. Your awareness of IBM’s data protection requirements will help you do your job. You will see that the proper handling of personal information goes to the heart of what it means to be a company built on Values, with trust and personal responsibility in all relationships.

Harriet Pearson
VP Regulatory Policy & Chief Privacy Officer
IBM Corporation
Privacy Self-Assessment Tool Flow

Intro / Welcome / Instructions → Authorized Process Selector → Country Selector → Prolog Questions

Assessment Questions → Gap Analysis Report → Exposures Report → Actions

Screeshots are from the pre-production global privacy assessment tool.
Global Data Incident Response Process: Objectives

1. Enable IBM to respond quickly and effectively to data security incidents involving personal information
   
   a. Enable early identification of incidents and a response which minimizes risk to affected individuals, meets regulatory obligations and protects the IBM business and brand
   
   b. Provide a mechanism by which the appropriate business leaders have support and necessary information to effectively manage such incidents

2. Identify trends and root causes behind incidents and use this learning to enhance IBM’s handling of personal information and response process
Conclusion & Discussion

- Global challenges require...
  - Integrated and values-based view
  - Understanding of bigger context
  - Prioritization
  - Technology can enable

- Getting privacy “right” is good business
For further information, contact…

Harriet P. Pearson
VP Regulatory Policy & Chief Privacy Officer
IBM Corporation
hpearson@us.ibm.com

P.S. You can find me on Facebook, Linked In, Plaxo and Xing. My office phone number is available on www.IBM.com. And, you can read more about me on Google.

P.P.S. Inside IBM, you can read my blog (CPO Blog) and find me on Beehive and Fringe (IBM social networking applications)