Privacy Management From a Practitioner's Perspective

PRIVACY SYMPOSIUM

Harvard University

August 22, 2007

Agnes Bundy Scanlan, Esq., Goodwin Procter
Michael Drobac, Chief Privacy Officer, Merrill Lynch
Joan Quinn, Privacy Compliance Manager, Bank of America

GOODWIN | PROCTER

TOTAL MERRILL

Bank of America

AGENDA

- Statutes & Developing Case Law
- The Practitioner's Challenge
- Open Forum

The A,B,Cs of U.S. Privacy Legislation

- GLBA (financial)
- HIPAA (health information)
- Federal Trade Commission Act (sec. 5)
- ECPA (electronic)
- CFAA (computer intrusions)
- FTC Act CAN SPAM Act (email marketing)
- FACTA

Gramm-Leach-Bliley

- Regulates disclosure of customer nonpublic personal information by financial institutions to nonaffiliated third parties
- Requires disclosure of policies, practices, descriptions of information that may be disclosed, must include opt-out options

Gramm-Leach-Bliley (cont.)

- "Privacy Safeguards Rule" governs security of personal information for our fund clients
  - Designate coordinator
  - Assess risks
  - Design program responsive to risks
  - Contractually require service providers to implement safeguards
  - Adapt program to account for material changes
- Pretexting provisions
  - Protect consumers from individuals and entities that obtain personal financial information under false pretenses

GLBA Enforcement

- FTC V. 30 Minute Mortage, Inc.
  - Defendants sold or offered to sell mortages to nonaffliated third parties without consumer consent
  - $57K fine and $1 million bond

- FTC v. 4086465 Canada, Inc.
  - Alleged that defendants masqueraded as government or bank officials and convinced consumers to disclose bank account information
  - FTC obtained TRO and froze defendant's assets

HIPAA

- HIPAA - Health Insurance Portability and Accountability Act of 1996
- Administrative simplification provision of the Act is to improve the efficiency and effectiveness of the health care system
  - Privacy and security standards to protect the confidentiality and integrity of individually identifiable health information
- All firms must consider this as it relates to employee benefit plans, etc.

Federal Trade Commission Act (sec. 5)

Prohibits “unfair or deceptive acts or practices” including acting counter to posted privacy and data security policies

- FTC v. Gateway Learning
  - Gateway promised it would not share information and then rented the info to target marketers
  - Gateway changed privacy policy mid-stream without notifying consumers
  - Gateway disgorged $4,600 earned in list rental
- In re MTS Inc. (Tower Records)
  - Company privacy policy claimed data was secure
  - data was vulnerable to hacking, however
  - Tower now required to undergo biannual web audits

Other U.S. Statutes

- ECPA (electronic privacy)
  - Electronic Communications Privacy Act (wiretap statute) prohibits interception and disclosure during transmission and Stored Communications and Transactional Records Act prohibits unauthorized access to stored communications
  - U.S. v. Councilman
- Computer Fraud & Abuse Act (computer intrusions)
  - Covers protected computers accessed without authorization or where exceeds authorization

Spyware Update

Federal Spyware bills pending

- HR 4661 - SPYWARE Prevention Act:
  - Criminal offense to access a computer without authorization and cause a program or code to be copied onto a computer to further another federal criminal offense, or to obtain or transmit PID or impair security protections on a computer
- Phishing provisions

Fair and Accurate Credit Transactions Act of 2003 (FACTA)

- Incorporates many consumer protections, including new tools to improve the accuracy of credit information and to help fight identity theft
- Provisions regarding general consumer rights
- Adds several responsibilities to companies that furnish information to the credit bureaus
  - Standards for accuracy of data maintained
  - Consumers are entitled to correct inaccuracies in data profiles
  - Consumers are entitled to opt-out of unsolicited offers

FACTA (cont.)

- Provisions regarding identity theft rights:
  - Procedures at credit bureaus to handle fraud alerts
  - Consumers are given the right to place fraud alerts on credit report and block credit bureaus from reporting information in their credit files as a result of identity theft

“CAN SPAM” Act

- Controlling the Assault of Non-Solicited Pornography and Marketing of 2003
- Effective date: January 1, 2004

Commercial Electronic Mail Messages

Definition: "Any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)."

Exemption for “transactional or relationship messages”

- A commercial email message the primary purpose of which is --
  - to facilitate or complete a previously agreed commercial transaction
  - to provide warranty, product recall or safety information
  - to provide notice of change in forms, features or account information
  - to provide employment information
  - to deliver goods and services

Case Law

- *In re BJ's Wholesale Club Inc.,* FTC File No. 0423160 (2005)
- BJ's engaged in a number of practices which did not provide reasonable security for sensitive customer information.
- BJ's: (1) failed to encrypt consumer information when it was transmitted or stored on computers in BJ's stores; (2) created unnecessary risks to the information by storing it for up to 30 days; (3) stored the information in files accessible by using commonly known default user IDs and passwords; (4) failed to use readily available security measures to prevent unauthorized wireless connections to its networks; and (5) failed to use measures to detect unauthorized access to the networks, etc.
- The settlement required BJ's to implement a comprehensive information security program and obtain independent audits every other year for 20 years.

Case Law, etc.

- *In the Matter of CardSystems Solutions, Inc.,* FTC Docket No. 052-3148 (2006)
- CardSystems kept information it had no reason to keep, and stored data in a way that put consumers' financial information at risk.
- CardSystems had insufficient passwords to prevent a hacker from taking control of its computers.
- Forty million credit card accounts were compromised.
- CardSystems settled the charges, was enjoined from any future violations of the Safeguards Rule, was ordered to implement a comprehensive security program, and was ordered to submit to an independent audit biannually for 10 years.

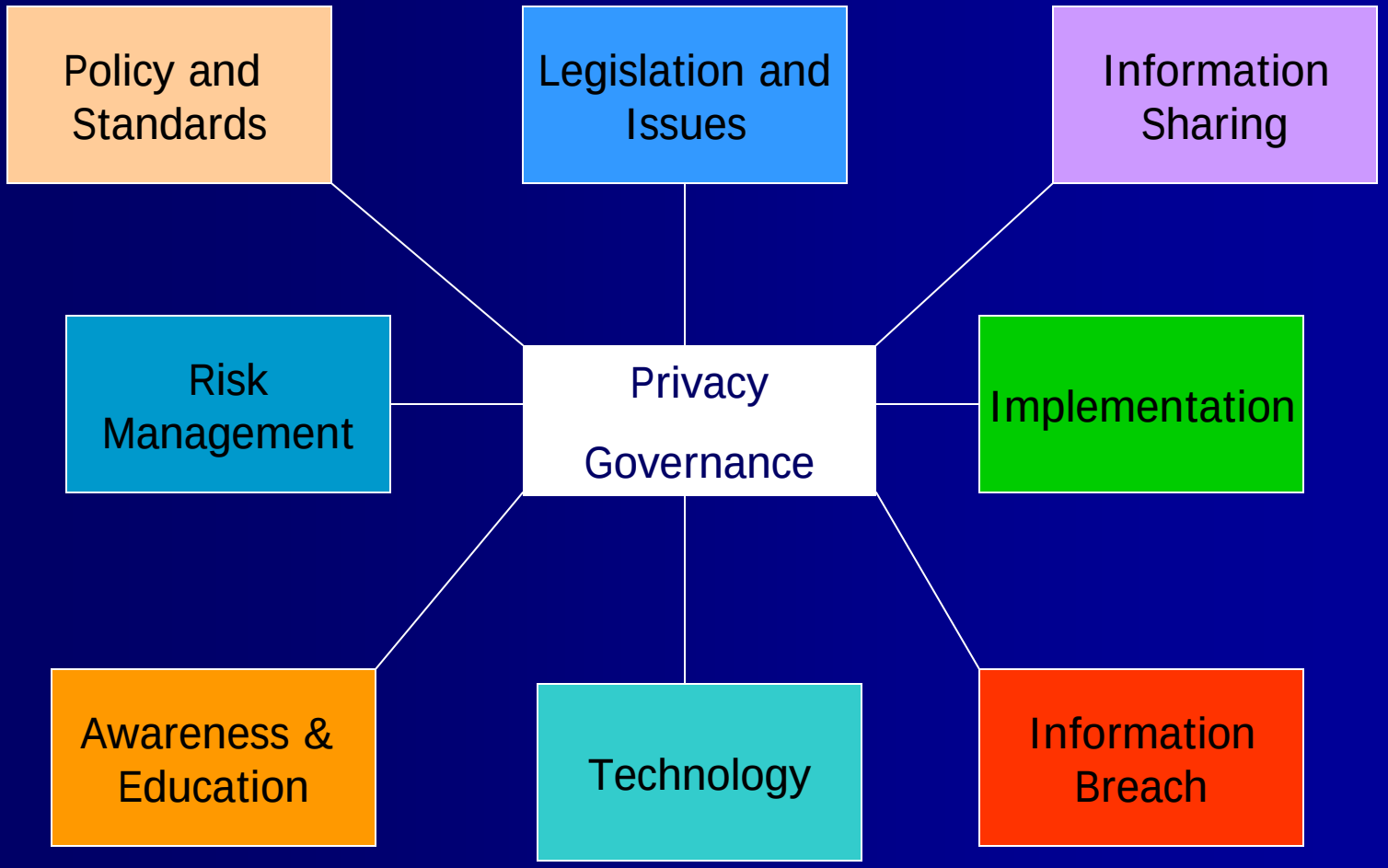
Case Law, etc.

- *TJX Company, 2007 (litigation pending)*
- Information from over 45 million credit cards "was compromised when a poorly secured wireless network" allowed hackers to obtain the data.
- Massachusetts Attorney General Martha Coakley is heading up the multi-state investigation.
- The FTC has indicated that it is investigating TJX.
- TJX also faces a class action lawsuit from over 300 banks. "TJX failed to protect customer data with adequate security measures, and TJX was not honest about how it handled data.
- The Arkansas Carpenters Pension Fund owns 4,500 shares of TJX stock and TJX denied its request to access documents outlining the company's IT security measures and its response to the data breach. The pension fund wants the records to see whether TJX's board has been doing its job in overseeing the company's handling of customer data.

Case Law, etc.

- *Victoria's Secret* (2003)
- The New York Attorney General claimed that Victoria's Secret exaggerated the level of privacy and security provided for the protection consumers' information.
- AG asserted that by failing to fulfill the pledge contained in its Privacy Statement, Victoria's Secret violated §§ 349 and 350 of the New York General Business Law which prohibit deceptive business practices and false advertising.
- In the 2004 Assurance of Discontinuance with the AG, the company agreed to improve its security, perform regular security audits, and pay $50,000 to New York State.

The Practitioner's Challenge



Policy and Standards

- Develop and update
  - ISO, AICPA, NIST standards
  - Coordination within enterprise
- Awareness
  - “Need to know”
  - Process changes/improvements
- Distribution
  - Global application
  - Local implementation

Legislation and Issues

- Impact analysis
  - Client
  - Corporation
- Influence
  - Lobbying
  - Role of industry groups
- Current issues

Information Sharing

- Affiliates
  - Consider FCRA, EU Directive, restrictions
- Vendors
  - Due diligence
  - Ongoing monitoring
- Third parties
  - Efficiently structured data flows

What's needed vs what's permitted vs <u>what the client expects</u>!

Implementation

- Dynamic arena requiring swift change
  - Weigh the cultural impact
- Management support
  - Take time with this group to ensure understanding
- Consider each of people, process, technology
  - Cross functional teams required to implement the most effective solutions

OPPORTUNITY FOR THE PRIVACY PRACTITIONER TO LEAD THE ENTERPRISE

Information Breach

- Event identification and process
- Notification standards
  - Differing requirements
  - Developing international position
- Trends and root causes
  - LESS technology, but process
  - Collaboration among industry & law enforcement

Technology

- Preference data base
  - Level (global, business unit, product)
  - Infrastructure
- Information access
  - Role based
  - Third parties
- Authentication

Awareness & Education

- Internal
  - Customized
  - Delivery method
- External
  - Customers
  - Others (regulators, business partners, etc.)
- Evaluation
  - Customer complaints
  - Surveys and benchmarks

Risk Management

- Compliance program
- Audits and examinations
- Issue management
- Monitoring
- New initiatives and emerging issues

Privacy Governance

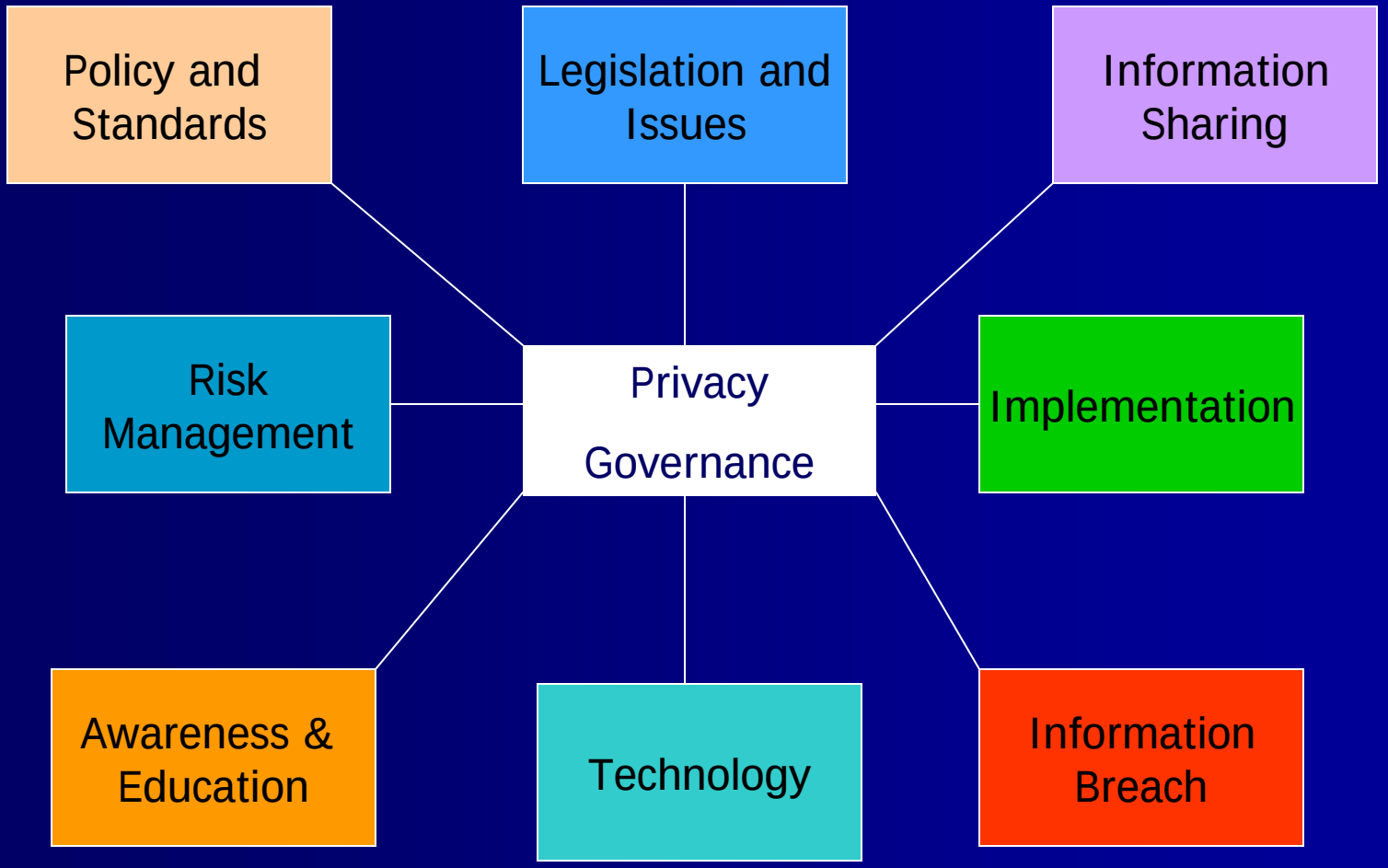
- Organizational structure
  - Must extend throughout the enterprise
  - Collaboration with other department heads
- Tools
  - Self assessments
  - Technological
- Metrics

GOVERNANCE results in INFLUENCE

Metric Considerations

- Policy & Standards
  - Exceptions: #'s, by business line...
  - Policy distribution #s vs. # new accounts open
- Information Breach
  - Time to resolve
  - Costs, including customer impact
  - Vendor-related
- Awareness & Education
  - New hire training: timing against standards
  - Customer complaints: #'s over time, root cause
- Access
  - Applications containing sensitive information
  - # of employees with access to sensitive applications

The Practitioner's Challenge



Privacy Management From a Practitioner's Perspective

Agnes Bundy Scanlan, Esq., Goodwin Procter
abundyscanlan@goodwinprocter.com 617-570-1161

Michael Drobac, Chief Privacy Officer, Merrill Lynch
michael_drobac@ml.com 609-282-2851

Joan Quinn, Privacy Compliance Manager, Bank of America
joan.b.quinn@bankofamerica.com 860-368-6066

GOODWIN | PROCTER

TOTAL MERRILL

Bank of America