Aligning RIM and Privacy for Effective Information Governance

Susan Goodman
MLS, IGP, CRM, CIPP/US, CIPM, CIP, ERMs, ECMp
February 9, 2016
BEC ARMA
Suegoodman.infogov@gmail.com
Learning Objectives

- Understand the Privacy landscape

- Explain the interfaces between Information Privacy and Records Management w/in the Information Governance Arena

- Play a critical leadership role in aligning, and sometimes leading, both functions in your organization to achieve compliance, reduce risk, and maximize opportunities related to information assets
Agenda

- Laying the groundwork:
  - The Information Privacy Landscape
  - RIM and Privacy within IG
  - How RIM and Privacy intersect, overlap and differ, and the value each brings to the other

- How to establish a strategic, tactical, and collaborative relationship between RIM and Privacy

- How to build a Privacy Program

- What’s right for you? Certifications, Employment Trends

- Links to Resources

- Summary/Questions/Discussion
Polling Questions

1. Demographics? RIM, Privacy, Legal, IT, Risk, Compliance, combination?
2. How many have seen a growing interest in Privacy in your organizations?
3. Those not representing Privacy - how many serve on a Privacy committee?
4. How many RIM professionals have increasing Privacy responsibilities?
What Data Must be Protected?

- **Personally Identifiable Information (PII)**
  - Identifies specific persons: customers, clients, employees, etc.
  - Sensitive financial information
    - E.g., payment card data (PCI)
  - Sensitive medical Information
    - Patient data
  - Other examples
  - Can depend upon information sources
  - Focus depends upon industry and regulatory entities
Privacy & Data Protection Models

- Comprehensive
- Sectoral
  - US/Japan
- Co-regulatory = GOV +
- Self-regulatory
  - Some in U.S. +
Privacy Frameworks

- Fair Information Practices (FIPs)
- OECD guidelines
- APEC privacy framework
- EU Data Protection Directive
- Generally Accepted Privacy Principles (GAPP)
- FTC’s Protecting Consumer Privacy in an Era of Rapid Change
- White House: Consumer Data Privacy in a Networked World
Examples of US Federal and State Privacy Law

- **US Federal Law – Examples (Plus Several bills introduced)**
  - Consumer Privacy Bill of Rights Act (2015) (Bill – introduced)
  - Data Security and Breach Notification Act of 2015 (Bill – introduced)
  - Right to Financial Privacy Act and GLB
  - Health Insurance Portability and Accountability Act (HIPAA) and HITECH
  - Family Educational Rights and Privacy Act (FERPA)
  - Children’s Online Privacy and Protection Act (COPPA)
  - Genetic Information Non-Discrimination Act
  - Telephone Consumer Protection Act
  - Fair Credit Reporting Act (FCRA), FACTA

- **State Law Typical Coverage**
  - Collection, use and processing, Information Security, Disclosure
  - Secure Disposal
  - Example: WA Public Records Act
  - MA and CA stand out
International Privacy Law

- In-Country/Cross Border Data Transfer
- EU Data Protection Directive
- Data Protection Act (GDPR) (New)
- EU-US Privacy Shield (New)
- Other Countries
- When Requirements Conflict
Typical Privacy Scope

- Preventing harm/rights of individuals
- Privacy policy and notice
- Collection
- Use
- Choice
- Data integrity
- Security
- Info life-cycle management
- Access and correction; explanation of refusal
- Accountability
- Transfer
- Enforcement
Key Players

- The White House
- Federal, provincial, state legislators
- Regulatory agencies
- State Attorneys General (US)
- The Courts
- Data protection authorities - EU, country specific
- Self regulatory/certification bodies
- International organizations
- Advocacy groups
- Professional/industry associations
### Expectations

<table>
<thead>
<tr>
<th>Expectation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comprehensive privacy program</td>
<td>“Say what you do/do what you say”</td>
</tr>
<tr>
<td>Privacy by design</td>
<td>Execute and monitor contracts w/ 3rd parties that maintain PII</td>
</tr>
<tr>
<td>Transparency</td>
<td>Gap in info security for PII can be considered unfair practice</td>
</tr>
<tr>
<td>Choice (e.g. tracking)</td>
<td>Lifecycle data management</td>
</tr>
<tr>
<td>Retention of PII for shortest time possible</td>
<td>Reportable incidents</td>
</tr>
</tbody>
</table>
Federal Trade Commission Focus

• FTC calling for:
  ▪ Privacy by design
  ▪ Simplified consumer choice
  ▪ Greater consumer control
  ▪ Transparency
  ▪ Increased information security

• FTC Focus Areas:
  ▪ The Internet of Things (IoT)
  ▪ Online Privacy (Online Tracking)
  ▪ Consumer Expectations
  ▪ The Economics of Privacy and Data Security
  ▪ Security and Usability
  ▪ Mobile Privacy
  ▪ Data brokers (e.g., “Big Data”)
  ▪ Large Platform Providers
  ▪ Promoting Enforceable Self-Regulatory codes
  ▪ Cross-border Data Transfer (Enhanced Role)

*From Jan 14 Privacy Con Event
Information protection and privacy has become a huge global concern affecting all businesses today, no matter their size, geographic footprint, industry, or ownership.

Headline news reports that data breaches are rapidly growing in number, frequency, and complexity. They are a huge risk for businesses.

Many of the data breaches experienced by the most sophisticated companies resulted from lack of basic precautions.
Why Invest? Risks & Consequences of Non-Compliance....

- Security attacks & data breaches
- Misuse of information / Identity Theft
- Regulatory investigations & sanctions
- Lawsuits
- Loss of Customers and Constituents
- Financial loss/Impact to Company Value
- Damage to Reputation and Brand
Other Benefits of a Privacy Program

- Compliance
- Trust (Customers/Constituents/Public)
- Cost Reduction & Avoidance
- Brand/Reputation Protection
- Competitive Advantage
- Enhanced Services
Information Governance Reference Model (IGRM)

Linking duty + value to information asset = efficient, effective management

**Duty:** Legal obligation for specific information

**Value:** Utility or business purpose of specific information

**Asset:** Specific container of information
RIM, Privacy & Information Governance

- Both part of IG
- Interdependent
- Increasing alignment
- Evolving and Maturing

w/in a Changing Landscape
Intersection of RIM & Privacy

<table>
<thead>
<tr>
<th>ARMA’s Principles / IG</th>
<th>Privacy Principles (e.g., GAPP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Accountability</td>
<td>1. Management</td>
</tr>
<tr>
<td>2. Transparency</td>
<td>2. Notice</td>
</tr>
<tr>
<td>3. Integrity</td>
<td>3. Quality</td>
</tr>
<tr>
<td>4. Protection</td>
<td>4. Security</td>
</tr>
<tr>
<td>5. Compliance</td>
<td>5. Disclosure to Third Parties</td>
</tr>
<tr>
<td>6. Availability</td>
<td>6. Monitoring and Enforcement</td>
</tr>
<tr>
<td>7. Disposition</td>
<td>7. Access</td>
</tr>
<tr>
<td>8. Creation and Retention</td>
<td>8. Use, Retention, and Disposal</td>
</tr>
<tr>
<td></td>
<td>9. Choice, Consent</td>
</tr>
<tr>
<td></td>
<td>10. Collection</td>
</tr>
</tbody>
</table>
RIM is Between 15-20% Privacy
Privacy is Between 15-20% RIM

- **RIM Teams:**
  - Create Records Inventories
  - Develop and apply retention schedules
  - Tag records w/requirements (including PII)
  - Ensure compliant RIM (e.g., retention/disposition) for ALL records - including PII and other sensitive information.

- **Privacy Teams:**
  - Create Privacy inventories
  - Identify and apply PII/PCI requirements and
  - Ensure compliant Privacy
What Privacy and RIM Have in Common

- Require management and controls

- Are evolving and maturing due to changing Legal/Regulatory environment and recognized complexities and risks

- Use / or are working toward an approach in keeping with information governance (IG) best principles and practices

- Support Legal, Compliance and Audit
  - Protect PII during Litigation, Regulatory Inquiry, Investigation
  - Conduct monitoring Audit; work with Audit teams
  - Support compliance with legal requirements for retention and disposition

- Support other teams: Information Security, HR, IT, Internal Audit
Commonality, Continued

- Develop data maps
- Perform, gap analyses
- Deal with big-data
- Apply regulatory requirements for records
- Are invested in information security
- Respond to data breaches and
- Ensure appropriate records/data disposition
Dependencies Between RIM and Privacy

- RIM is necessary to protect and manage personally identifying and sensitive information.
- Privacy requirements must be applied for compliant RIM.
- Each helps to ensure BOTH compliant RIM and compliant Privacy.

Understanding the Relationship is Key to Successfully Creating Functional Alignment
ARMA and the IAPP (AKA at an Industry Level)

• Growing recognition of this dependency and a trend toward the alignment of RIM and Privacy functions (e.g., scope of responsibilities).

• A strategic relationship developed between the key RIM and Privacy industry/professional associations

  • The International Association of Privacy Professionals (IAPP) and ARMA Intl.

*Encourage organizations you work with to collaborate*
What Will Your Privacy Role Be?

- Fostering Collaboration Between Privacy and RIM to Leverage Synergies

and possibly...

- Leading the Privacy Program

*Collaboration between RIM and Privacy is Critical in both scenarios....*
Aligning RIM and Privacy

• Communicating the synergies to all stakeholders

• Reviewing and integrating/cross-referencing policies, standards and procedures of the functions

• Tagging PII and other sensitive information in Retention Schedule and Electronic Records and Information Systems

• Working together to monitor/audit for compliance with information security, forward transfer (e.g., cross-border) and disposition/destruction requirements
Aligning the 2 Functions, Continued...

• Working together to monitor/audit for compliance with information security, forward transfer (e.g., cross-border) and disposition/destruction requirements

• Practicing collaborative decision-making

• Serving on each other’s committees

• Serving together on aligned teams: e.g., business continuity, HR (terminating /off-boarding employees), Legal/E-Discovery, etc.

• Conducting joint presentations
Tip 1: Gain Approval for a Privacy Program Development/Enhancement Initiative w/Resources

Tip 2: Complete Regulatory Review / Requirements ID

Tip 3: Conduct an Enterprise-Wide Privacy Inventory, Data Mapping, Policy Mapping, and a Needs / Gap Assessment:
   - Gather historical information - Privacy history: breaches, complaints
   - Measure current state (e.g., using AICPA Maturity Model, GAPP)
   - Determine Gaps, Business Needs, Competing Priorities, Perceived Risks
   - Complete a Risk Assessment: legal/litigation, operational, reputational, financial
   - Determine Actual and Desired Maturity Level and Target State

Tip 4: Conduct an assessment of controls for 3rd party/vendor risk for compliance with policies, processes, ongoing administration

Tip 5: Create a prioritized risk mitigation strategy and roadmap for moving to the desired state
Program Governance and Management

Components of Establishing the Program Infrastructure:

- The Business Case
- Mission and Scope – internal/3rd party
- Program Head (CPO)/ Privacy Team
- Program Governance including Privacy Committee and e.g., Information Governance Committee
- Privacy Policy and Notice
- Procedures and Controls, e.g., for
  - Regulatory Compliance
  - Opt-In, Opt-Out
  - Auditing vendor contracts and operations
Governance and Management, cont.

- Integrate Aligned Functions
- Reporting routines
- Monitoring and Auditing Compliance
- Roles and responsibilities for all stakeholders
- Technology – to track/manage program
- Technologies: Requirements for software and repositories that host PII
- Lifecycle management
- Privacy by design
- Data breach / Incident management
Necessary Components

- Governance and program management
- Privacy policy and notice
- Consumer choice
- Lifecycle data management
- Collection (including tracking), retention, protection, disclosure, and disposal
- Data quality/integrity
- Access and correction by data subjects
- Information/data security
- Breach notification
- Communications/training
- Monitoring and enforcement (internal; 3rd parties)
- Ongoing process improvement
Deeper Dive into Privacy Policy and Notice

- Privacy policy vs. privacy notice
- No material change w/out notice & consent
- Transparency/usability is key
- Make sure to “do what you say and say what you do”
- Challenges for mobile apps
Internal Communication & Training

- Develop an Intranet site for the Privacy Program
- Make Privacy Policy (and Notice if different) available to all staff
- Provide additional communication, procedures, etc. to departments responsible for PII with clear instructions
- Conduct staff training

- Use a Change management approach:
  - Continuous approach
  - Clear concise message
  - Builds on increasing awareness
External Communication

- Issue Privacy Notice and related communication (e.g., on web-site, mobile apps)

- Provide additional, contextual information if not included in Notice

- Establish relationships with external stakeholders (regulators, BBB, advocacy groups, internet user groups, external advisors, etc.) and industry/professional associations - to showcase your program and gain important advice and knowledge
Reducing Risk

- Close Gaps, Track and Monitor Compliance to Reduce Risk:
  - Work with departments to close gaps and mitigate risk
  - Work with Information Security, Risk to ensure that Privacy Program requirements are included in systems/processes
  - Monitor Compliance
  - Assess residual or new risk
  - Track PII disclosure in database
  - Track complaints and complaint resolution
Ongoing Process Improvement

- Identify needed improvements as resulting from:
  - Ongoing Monitoring
  - Data breach / incident issues
  - Audit / compliance failures
  - Changes in PII lifecycle
  - New or updated legislation/functions/requirements
Becoming Trained in Privacy

- Join IAPP
- Attend webinars, classes
- Purchase materials to assist (e.g., through IAPP and ARMA bookstore, webinars, conferences, Internet resources etc.)
- Network with Privacy Professionals
- Become Certified
Becoming a Certified Privacy Professional

- International Association of Privacy Professionals (IAPP)

- Three types of certification (and counting…)

![Certification Logos]
Certified Information Privacy Professional

- Laws/Regulations/Frameworks

- To be CIPP-certified, you must pass both
  - The Certification Foundation Exam and
  - A CIPP Concentration Exam
    - U.S. private-sector (CIPP/US)
    - Canada (CIPP/C)
    - Europe (CIPP/E)
    - U.S. Government (CIPP/G)

- The Foundation Exam must be passed first

- Cost: Several Hundred Dollars
Certified Information Privacy Manager

- Privacy Program Management/Operations
- Built on top of Privacy Foundation Program
  - Must first pass Privacy Foundations Exam
- Includes
  - Creating a company vision
  - Structuring the privacy team
  - Developing/implementing a privacy program framework
  - Communicating to stakeholders
  - Measuring performance
  - The privacy program operational lifecycle
Certified Information Privacy Technologist

• Built on Certification Foundation Program

• For IT professionals:
  • Privacy concepts/practices
  • Consumer privacy expectations/responsibility
  • Securing data privacy throughout the IT lifecycles
  • Privacy-by Design
  • Data collection and transfer
  • Pre-empting privacy issues in the Internet of Things
  • Factoring privacy into data classification and emerging technology
  • Communicating privacy issues
Summary and...

- Questions
- Comments
- Discussion

• Enjoy....
Links to Key Privacy Organizations and Certification Bodies

- International Association of Privacy Professionals: [www.iapp.org](http://www.iapp.org).
- TRUSTe: [www.truste.com](http://www.truste.com)
- Digital Advertising Alliance: [http://www.digitaladvertisingalliance.org](http://www.digitaladvertisingalliance.org)
- Electronic Frontier Foundation (EFF): [www.eff.org](http://www.eff.org)
- Electronic Privacy Information Center (EPIC): [www.epic.org](http://www.epic.org)
Links to Key Privacy Frameworks


- Payment Card Industry Data Security Standard (PCI DSS) [https://www.pcisecuritystandards.org](https://www.pcisecuritystandards.org)
Links to Several Privacy Initiatives/Publications

  - Marketing Your Mobile App: Get it Right from the Start (2012)


- Report to the President Big Data and Privacy, a Technological Perspective (2014)
  https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf

- Consumer Privacy Bill of Rights Act (2015) (Bill – introduced)

- White House, Consumer Data Privacy in a Networked World (2012)

- City of Seattle Privacy Initiative: http://www.seattle.gov/information-technology/privacy-program