Records Retention and Destruction Policy: Key Privacy and E-Discovery Implications to Consider

David L. Stanton
Pillsbury, Los Angeles
david.stanton@pillsburylaw.com
213-488-7271

Jenna F. Karadbil
Pillsbury, New York
jfk@pillsburylaw.com
212-858-1997

May 7, 2013

Topics for Today's Presentation

- Why should companies develop information governance programs?
- Key features of a proactive information governance program
- E-Discovery considerations
- Privacy considerations

What is Information Governance?

- "Information Governance"
  - The inter-disciplinary framework of policies, procedures and processes designed to optimize business value and to manage the costs and risks associated with information.
- IG Processes can include:
  - Retention and Deletion
  - E-Discovery
  - Privacy
  - Security
  - IT Systems Governance
  - Knowledge Management
  - Document Management
  - Business Continuity / Disaster Recovery
  - Storage Management
  - Enterprise Search

pillsbury

Why Bother? Developing the ROI for IG

- Cost Avoidance and Reduction
  - Hard Costs – storage and e-discovery
    - Immediately quantifiable
  - Soft Costs – search/retrieval and personnel
    - Lost productivity when users cannot find what they need
- Risk Management
  - Consider, e.g., data loss, privacy violations, security breach, harm to reputation, litigation risks
  - Can be quantified according to value of exposure (sanction, fine, adverse result) multiplied by likelihood of event.
- Optimization of Business Value
  - Improved availability enhances decision-making and customer experience
  - Recognition of information value aligns systems and strategies and drives process improvements

Key Elements of an Information Governance Program

- People
  - Independent Steering Committee
    - Legal
    - IT
    - RIM
    - Business
  - C-Level Support
- Process
  - Aim toward clearly defined objectives aligned with business strategy of the organization
  - Independence from department silos
- Technology
  - Integration of process improvements with organizational systems.

pillsbury

Early Steps Toward Information Governance

- Put a team together / solicit sponsorship / develop ROI
- Gather input and feedback from stakeholders
- Define the strategic objectives of the IG program
- Evaluate existing policies and procedures in light of defined objectives
- Assess existing legal holds and legal hold process
- Delete what you most readily can
  - Immediate savings
  - Success builds credibility and support
  - Obtain legal guidance and certification as to destruction
  - Consider less expensive alternatives for inactive data
- Target areas of greatest concern
  - Confirm or enhance security for confidential/sensitive information
  - Confirm retention of records having permanent value

Building a Robust Information Governance Program

- Specify and define business environments of greatest concern
- Catalogue information repositories / data mapping
- Determine existing retention methods and systems
- Research and schedule applicable legal requirements
- Design, draft and implement process Improvements
- Monitor, measure, maintain and update

pillsbury

Specification of the Business Environment

Identify:

- Business Lines, Departments
- Products and Services
- Types of customers served
- Geographic locations for customers
- Geographic locations of business

pillsbury

Cataloging the Information Repositories – Users

1. Laptop computer
2. External HD
3. PDA
4. iPod
5. USB memory stick
6. DVDs/CDs
7. Telephone
8. Desktop computer
9. Backup tape
10. Paper records
11. Sticky notes

Cataloging the Information Repositories - Enterprise

- Unstructured vs. Structured
- Useful vs. Obsolete
  - Customer data
  - Data from a divested asset
  - Legacy systems
- Information not subject to retention rules

Cataloging the Information Repositories – Mapping

- What types of records are created?
- Where is each type of record stored?
  - Geographic location
  - Physical machine vs. Hosted
- How is each type stored?
  - Functional vs. Category vs. Content
- What formats are used?
  - Hard copy
  - Electronic
    - customer data
    - business documents
  - Legacy systems
  - System data
- Who has control over each type of record?
  - Current responsibility for maintenance and destruction

pillsbury

Determine existing retention methods and necessary improvements

- Collect and review current policies
  - Retention/destruction policies and schedules
  - IT policies and procedures
  - Legal hold policy
  - Social media policy
  - BYOD
- Review enforcement and compliance infrastructure
  - How are the current policies and schedules enforced?
  - How are the current policies and schedules updated and maintained?
- Questions:
  - Are existing policies in alignment with the IG objectives?
  - Is routine disposal integrated into existing policies and practices?
  - Can policies or procedures be replaced with imbedded processes?
  - Are schedules media-independent? Are they current and complete?

Research and schedule applicable legal retention requirements

- Federal Electronic Signatures in Global and National Commerce Act (E-SIGN)
- Federal Insurance Contribution Act (FICA)
- Federal Unemployment Act (FUTA)
- Employee Retirement Income Security Act (ERISA)
- Equal Pay Act
- Occupational Safety and Health Act (OSHA)
- Fair and Accurate Credit Transaction Act (FACTA)
- Uniform Electronic Transactions Act (UETA)
- Federal Family Educational Rights and Privacy Act (FERPA)
- North American Free Trade Agreement (NAFTA)
- Sarbanes-Oxley Act (SOX)
- Gramm-Leach Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)

Research and schedule legal retention requirements

- Business specific regulations
- Geographic specific regulations
- Privacy regulations
- Statutes of limitations
- Customer contract requirements
- Media requirements
- Storage location requirements

Design, Draft and Implement Process Improvements

- Consider Existing and New Policies and Procedures
- Align policies and procedures with defined information governance objectives
- Empower the routine destruction of data with no value or legal need to retain
- Imbed categorization within technology as much as possible
- Training, training, training

pillsbury

Monitor, measure, maintain and update

- Determine in advance how you will you define success / KPIs
- Build accountability into the program
- Audit performance and compliance
- Schedule periodic review of rules and systems
- Ensure new technology is brought onboard in accordance with IG objectives

E-Discovery - the Basics

- Organizations of all types confront a series of costly tasks required to identify, process and produce information to support internal investigations and audits, lawsuits and regulatory requests.
- Unstructured data, including email and loose e-files, are the most common targets of e-discovery.
- The costs of e-discovery are proportional to the volumes of data that the process must consider. The more data that must be handled, the higher the costs.
- Poorly organized information can cause millions of dollars in avoidable e-discovery costs.
- According to the RAND Institute, merely reviewing a gigabyte of information for litigation can cost $14,000.

pillsbury

E-Discovery As A Component of Information Governance

- Improving e-discovery practices is one very achievable and practical objective of Information Governance
  - High costs
  - High risks
  - High value of targeted information in lawsuits
- E-discovery in is typically reactive; changing this is key
- The process components of e-discovery are repeatable business processes
- Delegation of e-discovery to trial counsel is inefficient; consider using discovery counsel

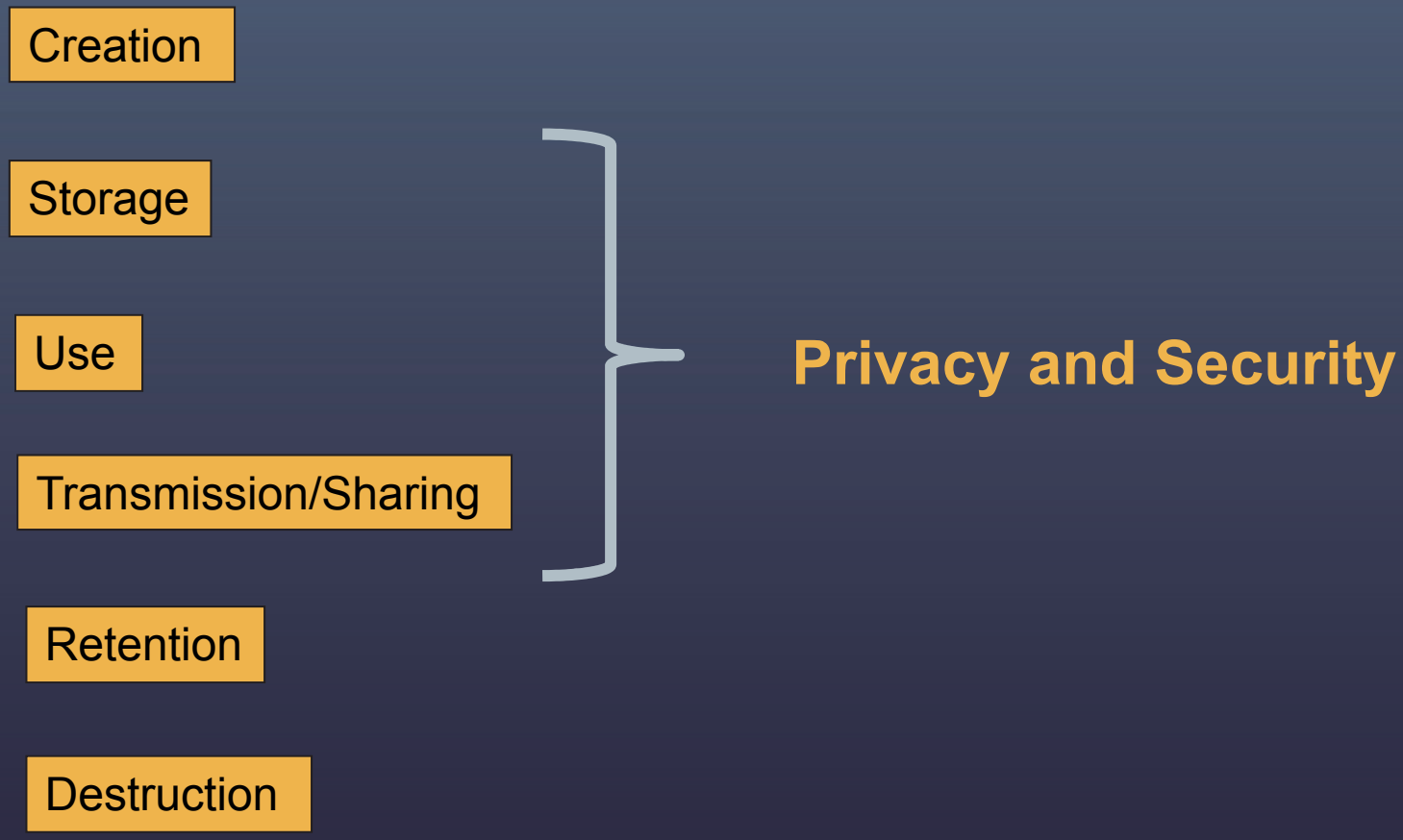
pillsbury

Privacy Concerns

- Content
- Confidentiality/Security
- Access
- Ownership
- Required Destruction/Disposal

pillsbury

Privacy in the information lifecycle



Privacy - Areas of Legal Protection

- No express US Constitutional protection
  - Some states constitutions, have express privacy provisions
  - California Constitution, Article 1, Section 1:

    "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."
- Industry self-regulation
- Federal legislation
- State legislation
- European legislation

Federal Privacy Protections

- Consumer Privacy
  - Federal Trade Commission
    - Deceptive trade practices, Unfair trade practices
    - Children's Online Privacy Protection Act (COPPA), CAN-SPAM
- Medical Privacy
  - Department of Health and Human Services
    - HIPAA
- Financial Privacy
  - Consumer Financial Protection Bureau
  - Federal Reserve
  - Office of the Comptroller of Currency
    - Gramm-Leach-Bliley Act (GLBA)
- U.S. / EU Data Transfers
  - Departments of Commerce and Transportation
    - EU Safe Harbor

Collection of Protected Private Information

- Identify the protected information collected and/or retained by the organization
- Understand and catalogue the state and federal laws that apply
  - Multiple states' laws may apply to your business
  - Both state and federal laws may apply to the same types of information
  - Must follow and adapt to the most restrictive rule
- Schedule the scope and types of collection and retention allowed

Consider:
Are you collecting more information than you actually need?

EU Privacy Protections

- Notice
  - subjects whose data is being collected should be given notice of such collection.
- Purpose
  - data collected should be used only for stated purpose(s) and for no other purposes.
- Consent
  - personal data should not be disclosed or shared without consent from its subject(s).
- Security
  - once collected, personal data should be kept safe and secure from abuse, theft, or loss.
- Disclosure
  - subjects whose personal data is being collected should be informed as to who is collecting it
- Access
  - subjects should granted access to their personal data and allowed to correct any inaccuracies
- Accountability
  - subjects should be able to hold personal data collectors accountable for adhering to all seven of these principles.

Global Regimes

Asia (General) – EU-style privacy law, APEC

Japan – EU-style privacy law

Canada – EU-style privacy law (PIPEDA)

Australia / NZ – EU-style privacy law

US – "Harm"-based, sectoral privacy law

China – EU-style privacy law

Mexico – EU-style privacy law

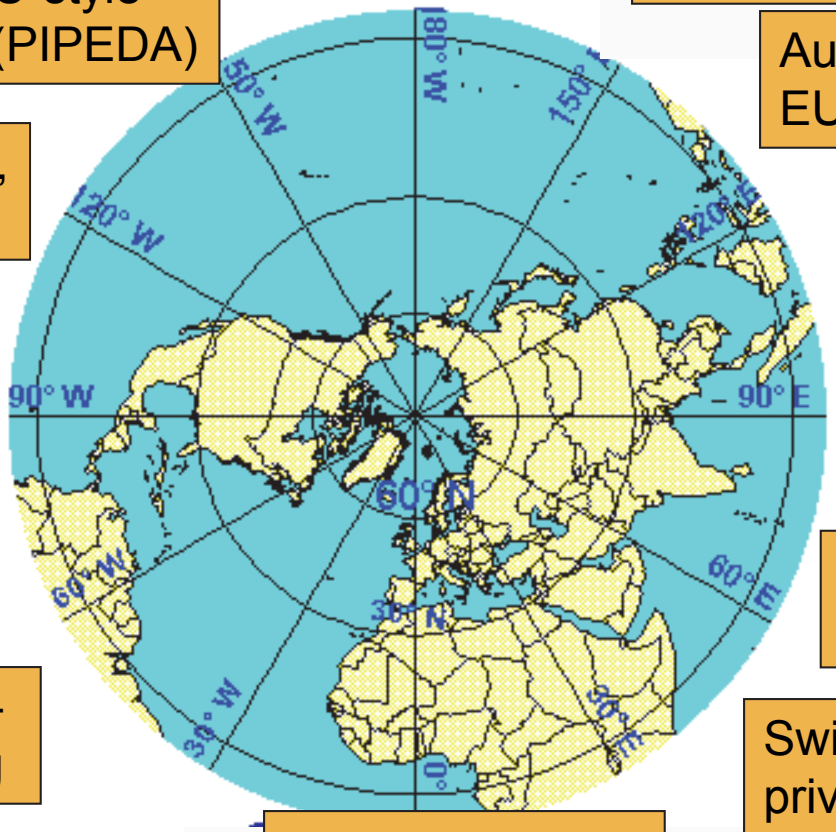
Russia – EU-style privacy law

Argentina – EU-style privacy law

EU – Most stringent privacy law

S. America (General) – Privacy law developing

Switzerland – EU-style privacy law



Dubai – EU-style privacy law. 1st in Middle East

Africa (General) – Privacy law developing

Israel – EU-style privacy law

pillsbury

Technologies Posing Key Privacy Concerns

- Backup tapes
  - Special dangers of backup tapes
    - Small size/high volume
    - Third-party storage
  - Examples
    - TRICARE/SAIC
    - New York hospitals
  - Ways to minimize risk
    - Training
    - Encryption

Technologies Posing Key Privacy Concerns (con't)

- Internet
  - Dangers
    - Customer registration and financial information
  - Examples
    - LivingSocial (50 million users)
    - Evernote (50 million users)
  - Ways to minimize risk
    - Strong passwords, additional protections (security questions, graphics)
    - Separate customer information across servers/databases
- Intranet
  - Dangers of using a company intranet system
    - Flip side of additional communication mode is risk of security
    - False sense of security raises risk of lax security measures
  - Example
    - TJX case—hacker attack accessed information regarding 450,000 customers
  - Ways to minimize risk
    - Rigorous security (strong and periodically changed passwords)
    - Separate HR information

Technologies Posing Key Privacy Concerns (con't)

- Laptops/Mobile Devices
  - Dangers
    - Most prevalent cause of data breaches
    - Extrinsic value makes them targets for theft
  - Examples
    - 2011 Sutter Health laptop theft > 4 million patients
    - 2009-2011 48 NASA laptops stolen
  - Ways to minimize risk
    - Encryption
    - Online tracking/remote wiping software

Technologies Posing Key Privacy Concerns (con't)

- Cloud Storage
  - Dangers
    - Loss of control of data
    - Dependence on third party for notification of breaches
  - Example
    - 2011 DropBox software bug made passwords optional for 4 hours
  - Ways to minimize risk
    - Provider segregation of your data
    - Breach notification procedures
    - Provider indemnification

Impact of Privacy Restrictions on E-Discovery

- Production of protected information in discovery is problematic
- Examples
  - HIPAA Privacy Regulation - Covered entity may disclose PHI:
    - With subject authorization
    - Pursuant to a court order
    - In response to discovery request if satisfactory assurances provided
  - GLBA – Financial institution may disclose protected information:
    - "to comply with federal, state, or local laws, rules and other applicable legal requirements"
    - to comply with "properly authorized civil, criminal, or regulatory investigation or subpoena or summons by federal, state, or local authorities"
    - "to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance or other purposes authorized by law
- Protective orders and redaction of protected information

pillsbury

Contact Details

David L. Stanton
Partner
Pillsbury Winthrop Shaw Pittman LLP
213.488.7271
david.stanton@pillsburylaw.com

Jenna F. Karadbil
Counsel
Pillsbury Winthrop Shaw Pittman LLP
212.858.1997
jfk@pillsburylaw.com