

# Time for Big League Play: Creative Solutions for Information Management

ACC Special Event CLE

Presented by

Nelson Mullins Riley & Scarborough LLP



Nelson Mullins

GLOBAL ISSUES

MEET & CONFERS

E-TRANSACTIONS  
E-ADMISSIBILITY

SECURITY/  
PRIVACY

HOLDS

RECORDS

ESI

VENDOR  
MANAGEMENT

# Records & Holds



- No ROI without RIM
- Consistency
- Holds
- Simplification
- E-Discovery Technology
- Policy Components
- Message Archiving
- Future ESI Challenges
- Tamper Detection

# No ROI Without RIM

## (Records & Info Management)

- The event-related expenditure of outsourcing e-discovery results in no process-related benefits, even in e-discovery, let alone in document, records and information management
- No storage cost savings
- No search cost savings or increases in search capabilities
- No organizing and retaining intellectual capital



# Consistency: Enter Ghost of Arthur Andersen

- AA records retention policy said client documents should be destroyed after an engagement concluded.
- Federal prosecutors said no partner or employee interviewed had ever known about or followed that policy.
- A “reminder email” concerning the policy was sent by AA counsel to AA’s Enron partners, and they began to destroy Enron documents.
- The Government’s case against AA was based in part on the fact that the policy had not been implemented by AA consistently.

“Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the party’s electronic information systems.”

(Rule 37(e) (formerly 37(f)))



# Holdings: Attorney Accountability for a Complex Compliance Process

- *In re NTL, Inc. Securities Litigation*, 244 F.R.D. 179 (S.D.N.Y. 2007)
  - “Although NTL sent out hold memos in March and June 2002 . . . those hold memos were not sufficient, since they subsequently were ignored by both NTLs. . . . The evidence, in fact, is that no adequate litigation hold existed at the NTLs.” (citing *Zubulake*).
- *Wachtel v. HealthNet*, 239 F.R.D. 81 (D.N.J. 2006)
  - Court criticizes HealthNet’s “utterly inadequate” eDiscovery process where paralegal merely emails preservation notifications.
- *Cache La Poudre Feeds, LLC v. Land O’Lakes, Inc.*, 244 F.R.D. 614 (D.Colo. 2007)
  - Court faults Land O’Lakes for simply directing employees to produce relevant information, and then **relied upon those same employees to exercise their discretion** to determine what information to save, rather than actively supervising a process

# Holdings, Records and Vendor Management

- Pension plan participants sought production of electronic pension plan records from the defendant employer.
- Defendant maintained it could not produce the data because it was in the possession of a third-party record-keeper.
- Plaintiffs argued that the defendant had a duty under ERISA to maintain the data for inspection or examination.
- Given the ERISA duty, the Court held the data was in the defendant's possession, custody or control within the meaning of Fed. R. Civ. P. 26(a)(1)(B) and subsequently ordered production of the requested documents.

*Tomlinson v. El Paso Corp.*, 2007 WL 2521806 (D.Colo. Aug. 31, 2007)

- Vendor obligations should be addressed specifically in the contract and SLAs, but even so vendor management participation in preservation teams and processes can be important.



# Information Management Team, for Issues from Holds to Vendor Management

- Legal
- Information Technology
- Human Resources
- Compliance
- Records Management
- Security
- Procurement/VMO/Finance
- Risk Management



# The Big Changes in Records Management Programs Now

- Your old record retention schedule was designed for a much smaller volume of more structured paper, based on regulations
- Can you expect all employees who touch messaging to comply with every regulatory time period solely through manual filing?
- But the records management programs are changing:
  1. **Simplification** ("big buckets" based on risk and cost-benefit considerations)
  2. Integration with enterprise content management (ECM) strategy
  3. Training/audit/monitoring/enforcement
  4. Technology for search/organization/de-duplication
  5. Hold processes and technology
  6. Technology and processes to assure authenticity of eRecords

# Top 6 E-Discovery Process/Technology Needs are Very Similar

1. Defensible searchability through automated processes to the maximum extent cost-effective, with audit trails
2. Defensible, consistently-applied record and document retention and destruction policies, processes and technology, with audit trails
3. Procedures/technology for the authentication of eDocuments
4. Reliable hold processes and technology, with audit trails
5. 26(f) readiness
  - where the relevant information can likely be found
  - how it can be produced, how quickly, and in what form
  - clear, defensible distinctions between accessible and inaccessible documents (26(b)(2))
6. “Project management” software/processes to make sure proper steps are followed and documented

# Key Components of a Records Policy Now



1. Policy document emphasizing accountability and the primacy of holds
2. Simplified, functionally-defined schedule
3. Hold Process
4. Roles and Responsibilities
5. Implementation and Administration
6. Imaging Process for E-Records
7. Separate but closely linked: Electronic Resources Policy

# Things to Consider in Purchasing and Establishing Rules for An Email Archive

- The archiving industry developed primarily due to SEC requirements that broker-dealers and investment advisers archive ALL e-messages for several years, which include a requirement of tamper-preventive technology
- For the great majority of businesses that are not subject to those requirements, how much email do you need to keep, and for how long (in the absence of a litigation hold or record retention requirement, of course)?
  - Filtering at the front end
  - Retention periods (for non-records) consistent with business needs
- You may need to authenticate the email as the original
  - Will non-“archive” processes and technology (such as “journaling” in Lotus Notes) give you sufficient bases for authentication?

# Challenges of ESI Beyond Volume and Cost

1. It is dynamic, meaning that it can change based on its context, it can be destroyed by merely turning a computer on or off, and it can be incomprehensible if separated from the system that created it
2. It may be dispersed by messaging systems to vast audiences around the world in seconds, challenging traditional notions of custody
3. Openness of systems permits access, modification, theft
4. Decentralization and distributed processing (SOA, SaaS, Virtualization) exacerbates 2 and 3
5. Changing technology and business transitions undermine carefully crafted architectures
6. Improved efficiencies change definition of reasonableness
7. However, content may be bundled not only with medium, but with policy enforcement

# Tamper Prevention vs. Detection

- Tamper-preventive technology such as WORM technology (used in email archives) encapsulates data reliably
  - Not self-authenticating and must have a chain of custody
- Tamper-detective approaches such as hashing algorithms allow for comparison to any trusted original or trusted hash values.
  - Do not require a chain of custody except for the original or trusted hash value or private key.



# Records & Document Management Top 10

Today's records and document management programs must:

1. Be simple, clearly expressed and well-suited to employee communication and training for front-end administrability
2. Involve search capabilities that are defensible for e-discovery purposes and meet business needs
3. Include monitoring and/or auditing to demonstrate consistency and good faith compliance
4. Filter out unnecessary content to an acceptable yet defensible degree
5. Rely on the right combination of “end-user” action, automatic processes and post-send records management staff activity



# Records & Document Management Top 10 (cont'd)

Today's records and document management programs must:

6. Not compromise speed or productivity
7. Permit secure storage, preservation and transmission
8. Be capable of adjustment by the company based on changing needs
9. Be well-integrated into overall information management strategy
10. Be cost-justifiable in relation to all alternative approaches

# Top 10 Legal Hold Cost/Risk Pitfalls

1. Lack of a systemic and repeatable process
2. Inconsistent or *ad hoc* litigation hold team membership
3. Failure to document all major steps taken
4. Unknowingly compromising metadata
5. Inadequate attention to chain of custody

# Top 10 Legal Hold Cost/Risk Pitfalls (cont'd)

6. Relying on legal hold notices alone for preservation
7. Relying on custodians to identify and/or collect responsive files and emails
8. Over-reliance on manual review
9. Collection methodology does not integrate with processing and review
10. Overcollection – increases cost and burden (indicator of no or poorly defined process)

# Privacy & Information Security



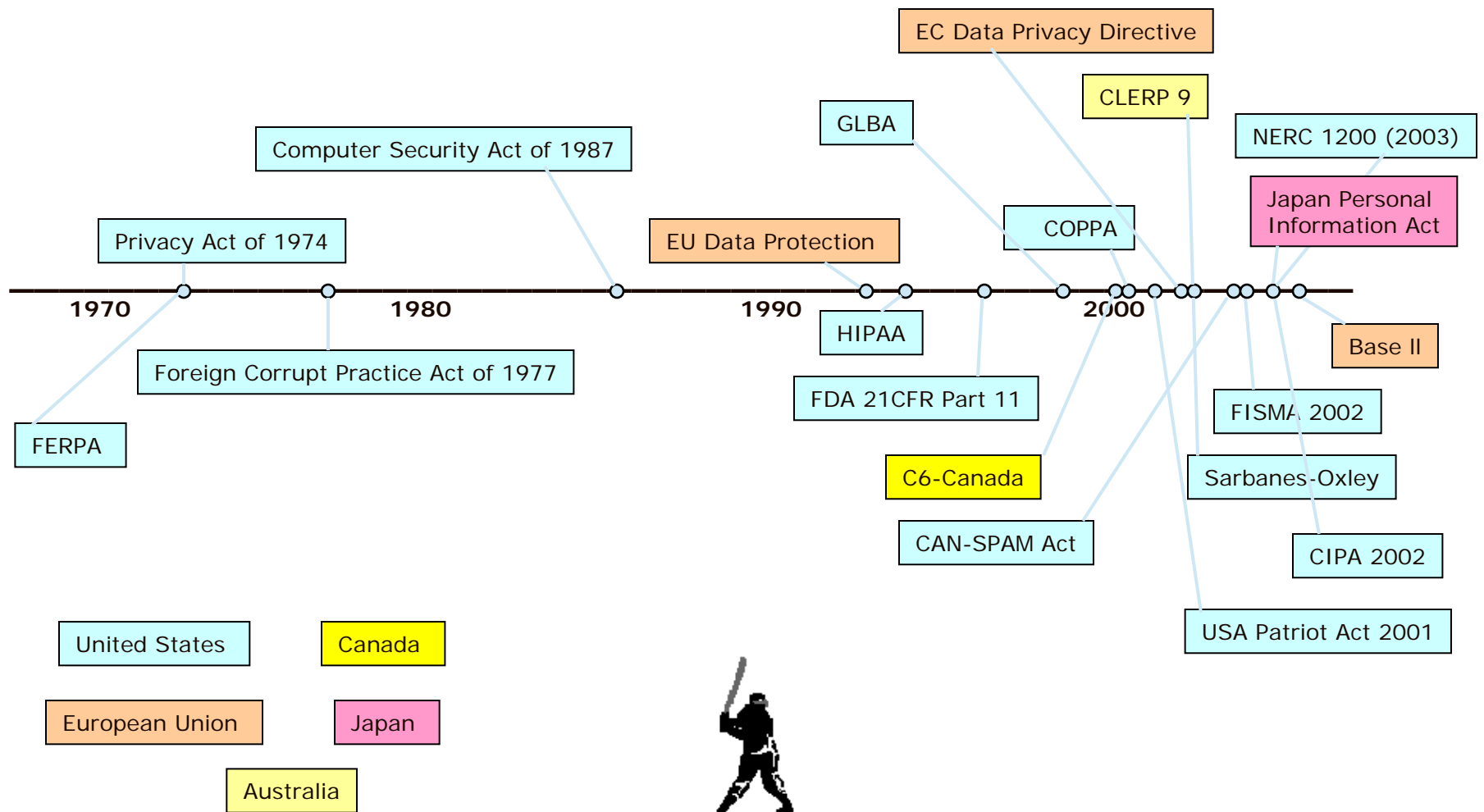
- Privacy Layers
- Security Layers
- The Public-Private Patchwork
- Breach Notification
- Most Important US Security Standards: PCI DSS & FTC
- Comprehensive Data Protection Laws
- CAN-SPAM Curve Ball

# Layers of U.S. Privacy Laws

- Fair Credit Reporting Act and FACT Act (now including affiliate marketing restrictions)
- Gramm-Leach-Bliley Act
- Employer Medical Privacy: HIPAA, GINA, ADA, FMLA
- Do-Not-Call Laws
- CAN-SPAM Act (New Final Rules effective July 7<sup>th</sup>)
- Anti-Wiretapping Laws
- Electronic Communications Privacy Act
- Privacy Act of 1974
- FTC Cases Regarding "Deceptive Trade Practices"
- Homeland Security Laws
- DPPA, COPPA, FERPA, plus laws re: SSN, AIDS, Mental Health, Substance Abuse, Domestic Violence, Genetic Testing....

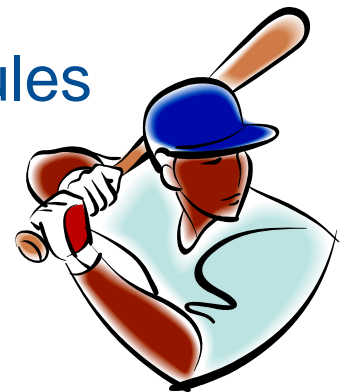


# Legislative Timeline: Acceleration



# Layers of Information Security Laws

- GLBA Safeguards
  - FTC Rule
  - Interagency Guidance Regarding Safeguarding and Regarding Unauthorized Access and Customer Notice (national banks)
  - Spreading beyond financial institutions under FTC's broad Section 5 consumer protection powers ("Unfair Trade Practices"), since 2004
- HIPAA Security
- State Breach Notification Laws
  - Have spread to almost all states
- Broad State Requirements of "Reasonable" Security for Personal Information (now 18 states)
- FCRA/FACTA: Disposal Rule and Red Flag Rules
- State Secure Destruction Laws
- Sarbanes-Oxley



# A Public-Private Patchwork

	<b>Private Enforcement</b>	<b>Regulatory Enforcement</b>	<b>Enforcement Through Competition</b>	<b>Court Enforcement</b>
<b>Private Standards</b>	e.g., Payment Card Industry Data Security Standard (PCI DSS), AICPA's GAPP, IIA's GTAG, ISO, ANSI	FTC enforcement of APEC Privacy Framework, HIPAA deference to WEDI, "deemers"	new privacy competition between ISPs, "best practices"	private and/or Government Standards become Liability standards
<b>Government Standards</b>	e.g., outsourcing and other vendor contracts (including HIPAA business associate contracts, GLBA service contractor agreements, EU contracts for data transfer)	e.g., GLBA enforcement by "functional regulators," FTC Act Section 5 authority, FCRA/FACTA	e.g., handling of breaches and provision of monitoring/insurance	e.g., e-discovery, attempts at security breach class actions

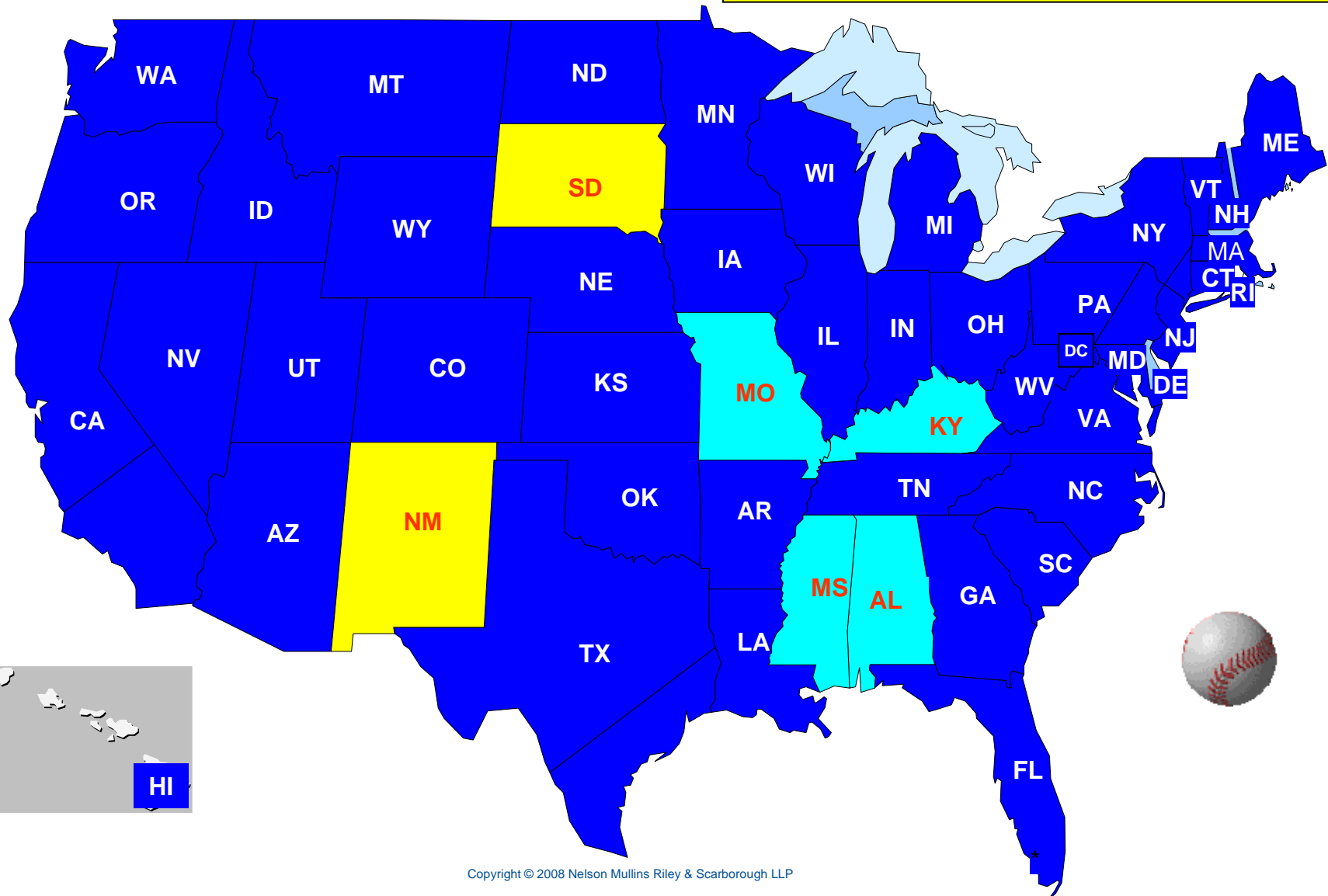
# Security Breach Notification Requirements



Security Breach Notification Bill(s) Introduced

Security Breach Notification Legislation Enacted

No Security Breach Notification Bills Introduced



# Some Important First State Law Questions in Dealing with Breaches

- Acquisition (or access) vs. harm
- All businesses vs. exclusions for privacy regulated entities or only “information brokers”
- Non-electronic data included?
- Personal information: The original California list vs. adding additional elements
- How soon notification must take place
- Report to authorities required?
- Law enforcement coordination exception?
- Pre-breach measures required?
- Civil/criminal penalties and/or private right of action

# Law-Driven Business Crisis, Not Regulation, Drives Security

- Consumer businesses may lose 20% to 30% of their customers that receive breach notices from them:
  - Only 8% of consumers who receive a security breach notification did not blame organization that sent the notice (usually the “owner or licensee”)
  - Over 40% said they might discontinue their relationship
  - Another 19% said that they had already done so
- Much higher percentage of employee breaches are notice-triggering
  - More SSNs
  - More medical information
  - More financial information

*Source: Ponemon Institute Surveys, 2005 and 2008 (30% is 2008 number)*



# Be Savvy About the Security Breach Industry

- Many forensics firms, PR firms and credit bureaus offer products that bundle breach-related services
  - Be very careful about listening to any vendor that has a financial interest in notification or other services
  - Make sure you get a quick, independent, expert read on legal requirements and whether and how notice should be given
- The great majority of breaches are not notice-triggering and may be addressed very quickly and inexpensively
- When breaches are notice-triggering, the quality of the communication matters
- Do not be misled about the value of notification or of credit monitoring to your customers and employees

# PCI DSS: Private Standards Drive Security



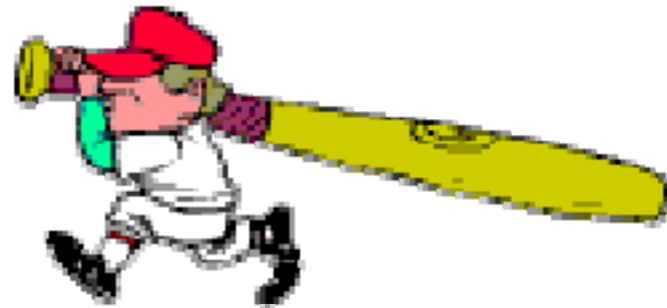
	Component	Storage Permitted	Protection Required	Encryption Required**
<b>Cardholder Data</b>	PAN	YES	YES	YES
	Expiration Date*	YES	YES	NO
	Service Code*	YES	YES	NO
	Cardholder Name*	YES	YES	NO
<b>Sensitive Authentication Data</b>	Full Magnetic Strip	NO	N/A	N/A
	CVC2/CVV/CID	NO	N/A	N/A
	PIN	NO	N/A	N/A

# FTC Case Law Drives Security

- Section 5 of the FTC Act prohibits unfair or deceptive acts or practices in or affecting commerce.
- A deception case requires a showing of three elements:
  - There must be a representation, practice, or omission likely to mislead consumers.
  - The consumers must be interpreting the message reasonably under the circumstances; and
  - The misleading effects must be “material” that is, likely to affect a consumers’ conduct or decision with regard to a product.
- A practice is unfair if:
  - There is substantial injury to consumers;
  - That is not reasonably avoidable by consumers; and
  - That is not outweighed by countervailing benefits to consumers or competition

# The FTC's "Best Practices"

1. Take Stock
2. Scale Down
3. Lock It
4. Pitch It
5. Plan Ahead



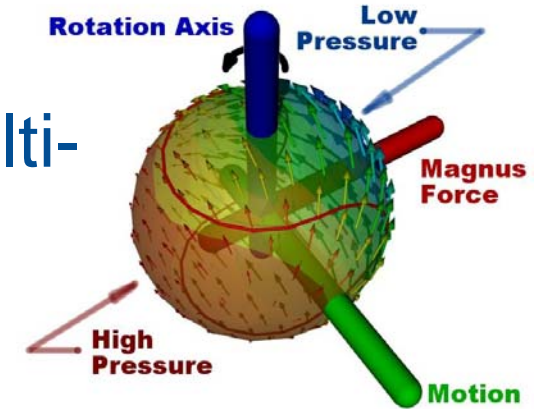
# EU Directive and Related National Laws

- Focuses on an individual's right of privacy rather than U.S. sectoral approach
- Restricts the processing of personal data and the flow of personal data outside the EU
- Directive sets the baseline requirements for data protection in each of the EU member states. Each member state is required to and has implemented legislation complying with the Directive
- U.S. Safe Harbor framework is designed to comply with the adequacy requirements of the Directive; 7 principles:
  - Notice
  - Choice
  - Onward transfer
  - Access
  - Security
  - Data integrity
  - Enforcement
- Other approaches to compliance, such as data transfer agreements, are also permitted by the EU



# Curve Ball: FTC's Latest Amendments to CAN-SPAM Act Regulations

- Effective July 7, 2008
- Clarify definition of "Sender" for multi-advertiser emails - single sender if:
  1. control content
  2. determine recipient email addresses
  3. identified as sender
- **Single web page** and no fee or other burden for opt-out right
- P.O. and private mail boxes acceptable
- CAN-SPAM covers nonprofits and others



# Privacy & Information Security Top 10

1. Privacy is closely linked to the ability to collect, manage, use and transfer valuable data
2. Information security demands regular broadly-focused risk assessments rather than neatly-tailored compliance audits
3. Start with your biggest risks. For most US entities, that means notice-triggering security breaches; try to prevent them, but be ready when they happen
4. Never forget vendor management; breaches of your information are usually caused by your vendors, and then you have the statutory obligation in most states to notify your customers/employees
5. Your requirements for personal information: privacy rules for its use and disclosure, and security processes and technology to protect and securely destroy it; not too bad when you know where it is

# Privacy & Information Security Top 10 (cont'd)

6. Educate your company's non-US-based affiliates on countervailing US law to their data protection laws (e.g., prevention of harassment/discrimination and e-discovery), and help them decide when and how to transfer customer/employee data to the US
7. Don't focus just on the obvious privacy laws; US privacy legal work involves many layers of overlapping and sometimes conflicting state and federal laws and private standards
8. The ISO information security standards and PCI DSS are the private standards that are becoming most influential
9. The most important general privacy/information security regulator in the US is the Federal Trade Commission, through both its rules and its case law on unfair and deceptive trade practices
10. Privacy and information security law is unstable, and information security risks even more so, so shake well before using "Top 10 Lists" like this one

# Electronic Transactions



- E-Signature Laws
- Creating an enforceable e-contracting process
- Beyond E-Signatures to E-Contracting, E-Archiving, E-Admissibility & E-Delivery

# E-Signature Laws

## E-signature Law

## Effective Date

Electronic Signatures in  
Global & National  
Commerce Act (ESIGN)

October 2000

Uniform Electronic  
Transactions Act (UETA)  
(adopted in all but NY,  
IL, Wash. & Georgia)

August 1999

# Electronic Signatures

- “e-Signature”: electronic sound, symbol, or process attached to or logically associated with a contract or record and executed or adopted with intent to sign the record.
  - Many different forms of e-sign technologies
  - Clicking “I AGREE” or saying “I AGREE”
  - One may sign electronically a tangible document
  - Can also use a voice signature to sign a “hard copy”

# Managing the Risks of Going Electronic

- Authentication Risk - Use “shared secrets” or other ways to affirm identity
- Repudiation Risk - Record the transaction, web or phone confirmations to establish what was signed
- Compliance Risk – Can more accurately confirm delivery of required documents electronically
- Usability Risk – How easy to use is it? Even low adoption may save plenty and increase customers. Include IM Team in design of process
- Enforceability Risk – E-contracts can be more enforceable than paper if process is sound; note, however, that contract principles (e.g., unconscionability, rules of evidence, fraud, etc.) still apply

# E-Signature Laws

More than just electronic signatures:

- e-sign
- e-contracts
- e-archive
- e-delivery
- e-admissibility

# E-Admissibility of eDocuments

- ***Lorraine v. Markel American Ins. Co.***, PWG-06-1893 (D. Md May 4, 2007). (101 Pages) Whenever electronic documents are offered as evidence, the party proffering the electronic information must consider the following:
  - whether the electronic evidence is relevant (Rule 501);
  - the authenticity of the information (Rule 901(a));
  - whether the information is hearsay, including relevant expectation, if the document is offered for its substantive truth (Rule 801);
  - the original writing rule (Rules 1001-1008); and
  - whether the probative value of the document is substantially outweighed by the danger of unfair prejudice or other considerations (Rule 403).

# Electronic Transactions Top 10

1. Electronic signature laws apply to electronic signatures, e-contracts, e-archiving, e-records and e-delivery
2. Generally state's UETA applies to intrastate transactions and ESIGN applies to interstate transactions, but ESIGN will preempt inconsistent state laws in NY, Georgia, Illinois and Washington
3. A digital signature is a type of electronic signature, but not equivalent to an electronic signature, which can be any sound, symbol or process
4. Designing an enforceable e-contracting process requires early and active involvement of IT, operations, legal, compliance and business at a minimum
5. Make sure document signed is what user saw, user's intent to sign was clear and that you can accurately recreate this document



# Electronic Transactions Top 10 (cont'd)

6. To address e-admissibility, design your e-signature process with a judge and the rules of evidence in mind
7. State and federal case law has permitted contracts originally in paper form to be amended electronically by email
8. All contract principles (e.g., unconscionability, fraud, etc.) continue to apply to e-contracts
9. Before original "hard copy" documents are destroyed after imaging, conduct a quality review and document your processes
10. For e-archiving, beware of orphaned data by ensuring continued availability and accessibility of e-documents following transition to new technology

# Vendor Management



- Real-World Info Mgmt
- Process
- Improving Traditional Provisions
- Building Vendor Mgmt into Info Mgmt

# Information Management for the Vendor-Reliant World

- Information management is relationship management, built on trust and communication
- Third-parties have increasingly important role to all organizations
- Why it matters for transactional lawyers to pull information management through their contracts
  - to consistently meet the service, quality, cost and satisfaction goals of the company
  - while mitigating new risks and protecting the company from liability

# When Information Management Can Be Critical

- Consulting Services
- Joint ventures and strategic alliances
- Licensing/Technology
- Logistics
- Outsourcing
- Procurement
- Other Vendor Arrangements

# Application of Information Management Practices to Vendors

1. Understand enough about internal information management programs
2. Identify desired service, quality, cost and satisfaction goals
3. Define and understand the process flow,
  - including transfer methodology, access, geographic transfer, and sensitivity
4. Assess unique information risks and identify gaps, e.g.:
  - interdependencies
  - insurance and risk management
  - regulatory
5. Re-check the validity of business case
6. Align stakeholders across the company around both expected benefits and risks
7. Develop a comprehensive plan to manage the risks over the process flow and term through risk management tools, technology, and appropriate contractual provisions

# Information Management Best Addressed Consistently from Day One

- Good vendor information management starts with the selection process
- Select the "right" vendor based on vendor information management capabilities and philosophy, alignment of desired performance goals and vendor strengths, company/vendor corporate cultures and existing infrastructures
  - The relationship is likely to be strategic and relatively long-term if it involves your information
  - Knowing how vendors handle information management and related compliance/contractual issues may enable streamlining processes (e.g., limiting RFI processes)
  - Due diligence regarding information management practices is critical
    - technical, administrative and physical controls
  - Engage in an open, early discussion of key terms beyond pricing, anticipating the interplay between information risk management and pricing/overall economics
- If the deal seems to be too good to be true, it probably is!

# Internal Due Diligence

- Understand the subject matter
  - Conduct an internal audit to understand the scope and depth of the processing activities and impacted data to be within the vendor's responsibility and the exposure involved
  - Identify foreseeable risks to security, confidentiality and integrity of customer, client, employee, and other data (unauthorized access, disclosure, misuse, alteration, and destruction)
  - Anticipate, plan and schedule the impact of the sourcing arrangement on existing internal resources and processes to ensure a smooth transition (necessary RIFs, knowledge management/transfer, transition)
  - Keep in mind there will be 2 transitions: outsource and eventual insource or resource (ensure some continuity and good knowledge repositories)
  - Anticipate integration issues with legacy systems, IT strategy, etc.

# External Due Diligence

- Know your vendor
  - Capabilities/experience
  - Communication/cooperation/culture
  - Financial stability/reliability
  - Track record/reputation (prior privacy complaints or investigations, lawsuits, security breaches, fines)
  - Host country environment and market
  - Host country legal and governmental protections
  - Infrastructure (methods used to protect and defend)

# Use Risk Management Tools Beyond the Contract

- Insurance products
  - including effective cyber-risk and other information management risk products
  - vendor or company as policyholders
- Extension of trusted internal processes
- Performance bonds
- Parent, U.S. subsidiary, "deep pocket" guaranty
- Solid back-up systems and up-to-date knowledge repositories

# Improving Traditional Remedies

<b>Traditional Remedies Meet Unique Need</b>	<b>Shortcomings</b>	<b>Alternatives</b>
Cure meets urgency of, e.g., breaches, privacy violations and holds	With data, vendor should perform a root cause analysis, but damage may be done	Focus should be on prevention with strong remedial options for company
Service Level Credits meet information performance expectations	While providing some cost relief, the impact on the vendor bottom line (and related role as a true performance incentive) is limited	In addition to structuring service level termination rights, build in financial performance opportunities for vendor
Termination meets operational requirements and more complex interdependencies	Usually not desired and a last resort given the cost considerations and impact on operations	Consider opportunity to terminate something of value to vendor (option to perform future services); allow termination of single SOW
Indemnification meets information protection requirements and risks	Limited to third party claims	Provide direct contractual remedies to mitigate potential direct damages
Change Control Process meets unforeseen information management events	Difficult to contemplate all scenarios that may impact value proposition over an extended term	Develop scorecards and implement benchmarking with specific remedies to couple with aggressive change control; require regular assessment of and testing against newly identified information threats

# Improving Traditional Contract Provisions

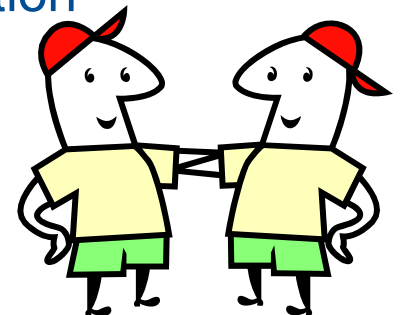
- **Governance** – While critical to any vendor relationship, governance provisions should be tailored to ensure that privacy, security and hold issues are handled on a timely basis, with proper notification and escalation
- **Knowledge management/repositories** – Impose specific requirements for process documentation (critical to maintain leverage and for an eventual exit)
- **Confidentiality protections** – Differentiate between "traditional" confidential information and sensitive/legally protected data (employee and customer) as the risks may be very different, including as they relate to the return/destruction, holds and meets and confers
- **Disaster recovery/business continuity/force majeure** – Address interplay and the need to expressly extend all security protections to an alternate hot site (technology, security, partitions)
- **Intellectual property** – While vendor may own IP rights in the technology, it is important to differentiate and protect company's ongoing ownership of all input/output data subject to the arrangement
- **Applicable security requirements** – Ensure compatibility between company and vendor information security policies, with clear contractual obligations as to the agreed standards (technical, administrative and physical (segregation/partition requirements))

# Improving Traditional Contract Provisions 2

- **Vendor personnel** – Special considerations apply due to access to the sensitive nature of the data – background check, training, retention of key personnel, general turnover issues, limitations under local laws and market considerations, right to and related process for subcontracting, assignment rights
- **Vendor representations** – Need specifics to address identified information-related risks and reliance on Internet transfer of data (reliability and accountability)
- **Compliance with law** – Data owner v. data processor responsibilities: laws may apply to one but not the other so "compliance with laws" boilerplate may fall short of providing adequate protection; additionally, avoid shifting the compliance obligations to the data processor but rather control the process (notification-related decisions) as the data owner and shift the costs of compliance to the vendor
- **Indemnification** – Traditional indemnification for third party claims will leave significant risks and related costs with the company around security and privacy compliance issues (regulatory fines, breach compliance costs).
- **Limited/excluded damages** – Traditional exclusions for certain types of damages may leave significant risk to the company as damages associated with a data breach may be indirect and therefore contractually excluded; as to monetary caps, there may be much more at stake than the value of the services provided so as to merit and justify a more creative approach to the existence and amount of any cap on damages.
- **Export Control** – Consider software/hardware location requirements and cross border transfers and related implications

# Managing Vendors Throughout the Relationship

1. Vendor managers must monitor performance daily, seek process improvements over time, and help the relationship evolve
2. Exercise your contractual rights – reporting, audit, service level accountability, escalation and documentation of all failures
3. Plan for and discuss the eventual exit; always keep break-up costs (financial, time and service) in mind
4. Ensure performance within statistically acceptable and agreed bounds; incentives should cut both ways to stand the test of time
5. It is important to keep the value proposition in place for the vendor to encourage continued engagement and provide a limited opportunity for the vendor to stray to other customers
6. Be creative as to both remedies and rewards; credits will not put enough on the line for the vendor to encourage continued service improvement
7. Integrate vendor management into the company's information management processes



## Time for a Vendor Change

- Similar to transition out to vendor; same care as for information flow analysis required
- Destruction and return of personal information can be critical, and must be confirmed
  - Identify and narrowly define vendor's legitimate needs, and assure effective protection of personal information kept
  - In a very recent incident, a massive data breach occurred in which a benefits vendor who should not have kept old employee records had a server stolen (didn't verify destruction; term provision suboptimal, company approached with massive bundled breach costs that we could drastically reduce)
- Termination assistance services/incentive, including effective and timely knowledge transfer

## Use the IM Team for Big Picture

- Team approach will prevent price driving the deal as long-term costs could quickly outweigh savings
- Define necessary internal resources at front and back end
- Present unified voice to management on priorities, planning and budgeting
- Manage system compatibility issues for the duration of the relationship
- Keep vendor management issues in front of the IM team

# Vendor Management Summary: Top 10 List

1. Understand the subject matter of the sourcing arrangement, including resources and information, information flow and vendor connections and interactions
2. Develop a vendor management program for your organization to ensure external application of relevant information-related policies, including security, background checks, document preservation and reporting obligations
3. Focus on data protection issues at the outset of the vendor negotiations
4. Establish and manage internal expectations for data protection and risk management issues and the importance of an ongoing monitoring and oversight program
5. Establish solid governance, reporting and knowledge management procedures



# Vendor Management Summary: Top 10 List (cont'd)



6. Plan for security breach issues and eventual exit
7. Understand the respective roles of owner and processor under applicable law and specifically address compliance-related concerns in the contract
8. Provide incentives to the vendor to achieve the business goals of the transaction while simultaneously managing information risks through insurance and contractual protections
9. Establish a process for changes driven by new laws and new threats, as well as advances in technology, associated with information management over the lifecycle of the outsourcing transaction
10. Implement appropriate and dynamic performance and remedial measures targeted specifically to ensure effective information risk management (e.g., credits, termination options and termination assistance)

# Questions? Batter up!

