MAYER·BROWN

Data Privacy Considerations When Conducting E-Discovery

Therese Craparo
Anthony J. Diana
Rebecca Kahan
Paul Chandler

May 17, 2011

Privacy & Data Security
Webinar Series on Privacy, Security and Data Protection

Mayer Brown is a global legal services organisation comprising legal practices that are separate entities ("Mayer Brown Practices"). The Mayer Brown Practices are: Mayer Brown LLP, a limited liability partnership established in the United States; Mayer Brown International LLP, a limited liability partnership (regulated by the Solicitors Regulation Authority and registered in England and Wales number OC 303359); Mayer Brown JSM, a Hong Kong partnership, and its associated entities in Asia; and Tauil & Chequer Advogados, a Brazilian law partnership with which Mayer Brown is associated. "Mayer Brown" and the Mayer Brown logo are the trademarks of the Mayer Brown Practices in their respective jurisdictions.

Speakers

Paul Chandler is a member of Mayer Brown's Business & Technology Sourcing practice in Chicago. Paul represents clients in connection with the outsourcing of information technology functions and business processes. In addition, Paul assists clients that are working to develop, license, market, distribute and acquire rights in a wide variety of technology-related products, services and intellectual properties, including computer software and hardware, databases, on-line services and telecommunications systems. He also represents clients interested in forming technology joint ventures and other strategic alliances.

Therese Craparo is a member of Mayer Brown's Electronic Discovery and Records Management practice. Clients rely on Therese to represent and advise them on all aspects of the discovery and management of electronic information including the development of policies and procedures for the preservation, collection, review and production of electronically stored information, the remediation of legacy data, and strategic positioning and defense of electronic discovery issues before federal regulators and the courts. She authored several chapters of Mayer Brown's *Electronic Discovery Deskbook*, published by the Practicing Law Institute, including chapters relating to preservation, third-party practice, and government and regulatory investigations.

Speakers

Anthony Diana, a partner in the New York office, focuses his practice on commercial litigation, electronic discovery, internal and regulatory investigations and bankruptcies. As a co-leader of Mayer Brown's Electronic Discovery and Records Management group, Anthony has counseled large financial institutions, pharmaceutical companies and manufacturers on all aspects of the discovery and management of electronic information, including: the development of policies and procedures for the preservation, collection, review, and production of electronically stored information; the development of data source catalogues, disclosures, and responses relating to electronically stored information; the remediation of large volumes of legacy data (paper and electronic); and the defense of electronic discovery procedures before federal regulators and the courts. Anthony is editor of the *Electronic Discovery Deskbook*, a treatise published by PLI, and co-author of six chapters in this treatise .

Rebecca Kahan is a litigator whose practice focuses on complex commercial litigation, including banking and financial services and electronic discovery. Rebecca is a member of Mayer Brown's Electronic Discovery & Records Management Practice. She counsels clients on various issues related to discovery and management of electronically stored information and has worked closely with clients and vendors to develop strategies for efficient collection, review, production and maintenance of that information.

Today's Topics

- Introduction to Data Privacy
- Business Sensitive Information and E-Discovery
- Data Privacy Concerns When Conducting E-Discovery
- Best Practices for Managing Data Privacy & Business Sensitive Information Risks
- International E-Discovery Issues
- Key Provisions in E-Discovery Vendor Contracts

Introduction to Data Privacy

- Data Privacy
  - The appropriate use of personal information under the circumstances.
  - What is personal information?
    - Sensitive information
    - Personally Identifiable Information (PII)
    - Protected Health Information (PHI)
    - Non-public personal financial information (NPI)

Introduction to Data Privacy

- Types of Personal Information
  - Name, gender, age and date of birth
  - Marital status, citizenship, nationality
  - Veteran status, disabled status
  - Personal address, phone number, email address, social media
  - Business address, phone number, email address, social media
  - Internal identification numbers
  - Government-issued identification numbers
    - Social Security number, driver's license, passport

Business Sensitive Information

- Business Sensitive Information (BSI) is Not "Private," But May Require Special Protections
- Types of BSI Subject to Special Requirements
  - Confidential Information
  - Trade Secrets
  - IP
  - Data subject to Non-Disclosure Agreements (NDAs)

Data Privacy Considerations When Conducting E-Discovery

- Data Privacy or BSI Concerns Are Often Overlooked in Litigation
- Potential Risks of Data Breaches with E-Discovery Increase as Scrutiny of Data Privacy Increases
- Federal Rules of Civil Procedure 26 & State Analogues Recognize that Protections May Be Necessary for Personal or BSI

Data Privacy Considerations When Conducting E-Discovery

- Information Life Cycle: Data Privacy & E-Discovery
  - Collect
  - Use/Process
  - Store/Retain/Archive
  - Disclose/Transfer

Data Privacy Considerations When Conducting E-Discovery

- Federal & State Laws
  - Gramm-Leach-Bliley Act (GLB Act)
  - Right to Financial Privacy Act (RFPA)
  - Health Insurance Portability and Accountability Act (HIPAA) & Health Information Technology for Economic & Clinical Health (HITECH) Act
  - Children's Online Protection Act (COPA)
  - Payment Card Industry Data Security Standards (PCI DSS)
  - State Privacy and Security Breach Laws
  - State Data Transfer Laws

Data Privacy Considerations When Conducting E-Discovery

- Relevant Regulatory Bodies
  - Federal Trade Commission (FTC)
  - Federal Communications Commission (FCC)
  - Department of Commerce
  - Consumer Financial Protection Bureau (CFPB)
  - Securities and Exchange Commission (SEC)
  - Federal & State Attorneys General

Best Practices for Managing Data Privacy & Confidentiality Risks in E-Discovery

- Understand where protected information resides
- Confer with requesting party regarding scope and implications of the request
- Consider use of protective orders, confidentiality agreements, government verifications, etc.
- Special protections when transferring data to law firm/vendor

Best Practices When Addressing Data Privacy & Confidentiality Risks in E-Discovery

- Procedures for collection, review and production
  - Limited collection, to the extent possible
  - Limited access to maintain status
  - Specific authorizations for release
  - Data Transfer (e.g., medium, encryption, FTP)
  - Additional review /quality control measures
  - Specific provisions in e-discovery vendor contract
- Special considerations when producing protected data (e.g., FOIA, stamping, markings, encryption)

Best Practices When Addressing Data Privacy & Confidentiality Risks in E-Discovery

- Special Considerations for NDAs
  - Contractual provisions requiring notice prior to production
  - Challenge of managing & organizing NDAs
  - Procedures for identifying relevant entities or individuals & relevant third party data
  - Procedures for notifying NDA counterparties

International Issues - Overview

- Discovery of Overseas ESI in U.S. Proceedings – Two Basic Inquires:
  - Do the Federal Rules of Civil Procedure require production of the overseas ESI: **possession, custody & control**
  - Does applicable foreign law permit the processing, transfer and production of the overseas ESI: **comity, hardship, diligence**
- The answers to these two questions are not always consistent.
  - Where available, Hague Convention procedures may help reconcile conflicting laws.
    - Time consuming process, narrower scope of discovery.

International Issues – Foreign Data Protection/Blocking Statutes

- Types of Foreign Laws that Serve as Potential Obstacles to Discovery of ESI
  - *Blocking Statutes*: Laws designed to protect sovereignty, and shield foreign nationals from intrusive U.S.-style litigation
  - *Data Protection Laws*: Laws designed to protect privacy – in some jurisdictions they cover broader categories of data than U.S. privacy laws
  - *Others*: PRC State Secret Laws, Bank Secrecy Laws, etc.

International Issues – Foreign Data Protection/Blocking Statutes

- Overview of European Union 1995 Data Protection Directive (Currently Under Review)
  - "Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to processing of personal data."
  - Directive restricts the processing and transfer of personal data
  - These terms are broadly defined
  - Provides for notice to affected employees, including target of an investigation
  - Implemented differently in each EU member state

International Issues – Foreign Data Protection/Blocking Statutes

- EU Directive: Practical Implications of "Legitimate Interest" Exception
  - WP 158: Exception only applies where legitimate interests are not "overridden by the interests for fundamental rights and freedoms of the data subject"
  - To minimize potential exposure, processing party will need to show "proportionality" of data processing, "relevance" of the personal data, and implementation of safeguards to protect personal data
    - Early filtering to minimize quantity of personal data involved
    - Redaction/anonymization
    - On-site/in-country review

International Issues – Foreign Data Protection/Blocking Statutes

- EU Directive: Transfer to U.S.
  - "Legitimate Interest" exception applies to processing only, not to transfer
  - Possible steps to permit transfer of data
    - Elimination of "personal data" from set transferred
    - Use of "safe harbor" vendors
    - Model contracts/strict protective orders
    - Hague Evidence Convention

International Issues – Foreign Data Protection/Blocking Statutes

- Data Protection Outside the EU
  - Outside the EU, data protection law is rapidly evolving, an the EU Directive is a leading model
    - Important to get country-specific, current advice from local counsel
  - For example, in Asia, data protection laws are not (yet) generally as onerous as the EU Directive, but there are other obstacles to discovery
    - E.g., PRC State Secrets protection
      - Protects data deemed to be “state secrets”
      - Broad implications in light of level of state involvement in economy

Key Provisions in E-Discovery Vendor Contracts

- E-Discovery vendors process and store BSI & personal data
  - Often very high-risk/highly sensitive data
- Traditionally, e-discovery vendor selection and contracting not subject to scrutiny
  - Selected by law firms without necessary due diligence
  - Litigation time pressure weakens customer bargaining power
  - Tended to be very vendor favorable

Key Provisions in E-Discovery Vendor Contracts

- Best practices:
  - Analyze available offerings and conduct a rational contracting process to enhance value
  - Treat e-Discovery services as important to the organization and plan accordingly
  - Remember: if the e-Discovery vendor discloses data, the customer may be liable
    - Use the contract to incentivize proper performance

Key Provisions in E-Discovery Vendor Contracts

- Typical Contract Structure:
  - Master Service Agreement
    - Governs relationship
  - Statements of Work (SOWs)
    - Customize SOWs to accommodate issues in particular case
      - Specific data privacy issues
  - Service Level Agreements

Key Provisions in E-Discovery Vendor Contracts

- Critical issue -- Protecting the data
  - Information Security Requirements
  - Prohibitions on Sub-contracting
  - Restrictions on data location
  - Confidentiality Provisions – limits on disclosure and use
    - Specific protections for most BSI
  - Right to access the data

Key Provisions in E-Discovery Vendor Contracts

- Critical Issue -- Protecting the data
  - Personal Information provisions
    - Specific protections for protected personal information
    - HIPPA/HITECH Compliance
      - Designation as “Business Associate”
    - European Data
    - Require compliance with future requirements
  - Notice of adverse impacts – e.g., actual or suspected breaches
  - Audits

Key Provisions in E-Discovery Vendor Contracts

- Warranties and indemnities
  - Data security breaches
  - Compliance with data privacy and data protection laws
  - Appropriate remedies
- Termination rights
  - Disposal or return of data
  - No withholding of data
  - Right to termination assistance – including getting a copy of the data in a usable format

Key Provisions in E-Discovery Vendor Contracts

- Other issues:
  - Continuity of Services during disputes
  - Limited vendor termination rights (e.g., only for non-payment of undisputed amounts)
  - No right for vendor to suspend services or withhold access to data
  - Detailed transition plan/implementation project details

Questions?

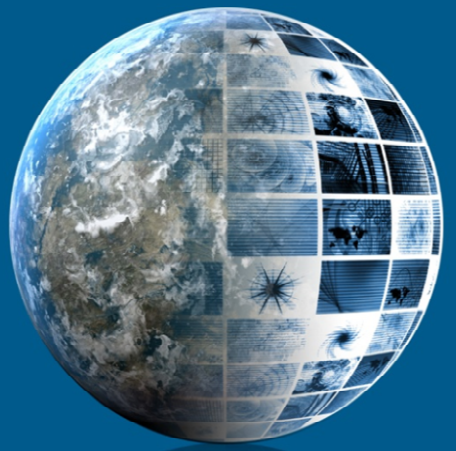
Paul Chandler
Counsel
+1 312 701 8499
pchandler@mayerbrown.com

Therese Craparo
Associate
+1 212 506 2312
tcraparo@mayerbrown.com

Anthony Diana
Partner
+1 212 506 2542
adiana@mayerbrown.com

Rebecca Kahan
Associate
+1 212 506 2229
rkahan@mayerbrown.com

MAYER·BROWN



Privacy & Data Security

Webinar Series on Privacy, Security and Data Protection

Mayer Brown is a global legal services organisation comprising legal practices that are separate entities ("Mayer Brown Practices"). The Mayer Brown Practices are: Mayer Brown LLP, a limited liability partnership established in the United States; Mayer Brown International LLP, a limited liability partnership (regulated by the Solicitors Regulation Authority and registered in England and Wales number OC 303359); Mayer Brown JSM, a Hong Kong partnership, and its associated entities in Asia; and Tauil & Chequer Advogados, a Brazilian law partnership with which Mayer Brown is associated. "Mayer Brown" and the Mayer Brown logo are the trademarks of the Mayer Brown Practices in their respective jurisdictions.