



Complying Across Continents

Electronic Discovery and Privacy Issues

Milton Luoma and Vicki Luoma
Complying Across Continents
H5 April 28, 2008



Worldwide

- Electronic Discovery differences between U.S. and Europe, Asia, Australia, New Zealand
- Privacy Law differences between U.S. and Europe, Asia, Australia, New Zealand
- Concerns of Multi-National Corporations

Federal Rules of Civil Procedure Rule 26:
E-Discovery U.S. Version

- Permissive: “Any matter not privileged that is relevant to the claim or defense of any party.” F.R.C.P. 26 (b) (1)
- Relevancy: “Relevant information need not be admissible at trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.

Zubulake v. UBS Warburg and
aftermath

- Balancing test for costs
- U.S. e-discovery will be a \$US5 billion in products and services by 2011

Common Law: United Kingdom

- In England individuals have the right to request any information a company may have pertaining to them, and then request that the company delete all of their personal information.
- They can also request a report on all disclosures of their protected information.
- A company's data-privacy and records-retention policy must remain consistent and enforceable to prevent any type of privacy breach.
- Personal Data Protection Bill

Canada

- Judge must determine at court whether the document is relevant or irrelevant.
- The party who makes disclosure must pay for the disclosure, unless the parties agree or a judge orders otherwise.
- Presumption of full disclosure
- The party who seeks to rebut the presumption must fully disclose the party's knowledge of what evidence is likely to be found or acquired if the disclosure obligation is not limited.
- The party who refuses a demand for access to electronic information must give reasons for the refusal, and the other party may move for an order under the rules.

Australia



- Australia adopted new e-discovery rules in December 2007 based on U.S. Federal Rules of Civil Procedure
 - Lawyers and relevant personnel will be required to work through the electronically stored information in a non-adversarial way.
 - This is expected to drive an explosion in the e-discovery business.
 - Australia is one of the most heavily populated countries in terms of computer users.
 - Kroll On Track opened offices in Australia and Japan.

New Zealand

- Law for Government
- Separate files for personal data versus company data
- Less litigious country



Japan



- Offers more protection for personal data or has broader definitions of what is considered personal data
- Discovery is extremely limited in Japan
- Companies often use technologies in order to evade discovery

China, Russia, India

- Electronic Discovery is very limited in China
- Electronic Discovery is also very limited in Russia – Russian Electronic Digital Signature Law
- India: Electronic Commerce Support Act, 1998; Information Technology Act in June 2000; United Nations Commission on International Trade Law (UNCITRAL) Model Law on eCommerce

Results in Global Differences

- United States litigants are often frustrated and feel hindered in the legal process outside of the United States.
- Litigants and companies outside the United States are barraged by the legal requirements of the United States.



Global Privacy Law



U.S. Privacy Laws

- General and decentralized
 - FTC
 - Electronic Communications Protection Act
 - Federal Regulations
 - State Consumer and Fraud Acts
 - Privacy Notice Requirements
 - Data Breach and Notification Laws
 - Labor and Employment Privacy Regulations
 - Sector Specific
 - Gramm-Leach-Bliley Act
 - HIPAA



European Privacy Framework



- EU Data (European Union Privacy Directives) provides Standards Valid in 25 EU countries
- Wide range of enforcement among the 25 countries
- Interpretations are inconsistent
- Personal data (data which identifies or concerns a named individual) cannot be transmitted outside the European Economic Area (the E.U. nations plus Iceland, Norway and Lichtenstein) to a country which does not provide, by national law, protection commensurate with the E.U. (Canada and Argentina are the only two countries)

EU Data Directive

- All computer processed personal data ...
 - Must have freely given consent
 - Individuals have absolute right to access data concerning themselves
 - Use must and processing must be lawful and fair, adequate, relevant and accurate
 - Must discontinue as soon as no longer necessary and adequate security must be in place
- All countries must have enforcement body in place
- Other countries must have Data Protection Agreement
- Discovery only allowed if party can show document exists and is key to the litigation

Japan

- Japan outsourcing of data processing services is permissible and service vendors may transfer data without consent, so long as they enter into an agreement with the data importer to protect the data.
- There are strict guidelines with eleven different ministries share responsibility for administering PIPA.
- Violations of PIPA may result in a fine of up to 300,000 yen (approximately \$2,500) or imprisonment for up to six months.

Personal Data Transferred Outside EU

- Must have “Adequate Protection.”
- France and many countries have criminal statutes
- Must be with permission or be permissible
 - Contractual arrangements
 - Third-party contract in interest of employee
 - Legal claims

Hague Option

- Hague System—One solution is for parties to request courts to invoke the Hague Convention on the Taking of Evidence Abroad in Civil and Commercial Matters
- Courts are often reluctant to grant such a request.
- American courts should ... take care to demonstrate due respect for any special problem confronted by the foreign litigant on account of its nationality or location of its operations, and for any sovereign interest expressed by a foreign state.

- Leading case of *Societe National Industrielle Aerospatiale v. United States District Court for the Southern District of Iowa*

Problems with Electronic Data

- Requirements around data privacy are having a big impact on how records are managed.
- Organizations must know what types of personal information they have and, most importantly, keep it secure.
- A company's data-privacy and records-retention policies must remain consistent and enforceable to prevent any type of privacy breach.
- Common universal problem – employees like to save information, often to protect their own self-interest.

International Data Collection

- The international issues are just starting to surface, such as the differing retention regulations here and abroad that affect the ability to collect and preserve relevant materials, and the concerns when litigating abroad under a foreign regulatory scheme.
- These conflicts raise both ethical and security risks that occur with outsourcing.

Third Restatement of Foreign Relations Law

- **Balancing Test**
 - Importance of documents
 - Specificity of request
 - Origination of document
 - Alternate means to secure information
 - Importance of competing state interests
- **Comity**

Data Protection

- Canadian – PIPEDA
- UK –Data Protection Act
- Germany - Federal Data Protection Act
- Mexico - E-Commerce Act
- Japan - Personal Information Protection Act
- Australia - Privacy Act 1988
- EU - EC Directive 95/46/EC

Develop Policies

- Develop a global record-retention policy and schedule based on the top five business drivers:
 - compliance
 - data privacy
 - litigation readiness
 - end-user needs
 - costs
- Address country-specific requirements on an exceptions basis
- Secure the privacy data and limit access to personally identifiable information.
- Conduct periodic audits to verify compliance
- Automate when possible

Company Decisions

- Review regulations in all possible jurisdictions
- Preparation is important
- Comply with as many as possible
- Set up Strategic Plan
- Separate Organizations and Processes
- Keep Duplicate data sets in various locations