Stormy Digital Weather Ahead: The Forecast for Cross-Border eDiscovery in the Context of Litigation and Regulatory Investigations

JAYNE ROTHMAN ESQ.
Vice President, Corporate Counsel, Epiq Systems, USA

ALISON WISNIEWSKI ESQ.
Senior Counsel, Epiq Systems, USA

M. JAMES DALEY, ESQ., CIPP/US
Co-Founder, Daley & Fey, USA

&

LAURA CLARK, ESQ., CIPP/US
Co-Founder, Daley & Fey, USA

We live in a digital world. Today, information is power, and electronically stored information (“ESI”) is its global currency. It is a world where well over 90% of information is created, transmitted and stored in electronic form. And it is a world where email, instant messaging, mobile devices and social media platforms such as Facebook® and Twitter® have become the lifeblood of corporate communication and collaboration. These platforms frame how organizations do business; they impact virtually every major corporate decision and action that might be the future subject of civil or criminal scrutiny.

This article examines the clash of cross-border discovery with global data privacy and protection laws, and the perfect storm that it can create for compliance. It also attempts to forecast the stormy digital weather ahead for international in-house counsel by examining some of the major challenges of navigating these conflicting and competing forces.

For organizations worldwide, digital information is ubiquitous—it proliferates and replicates at lightning speed, literally “bit-by-bit.” Thyroff v. Nationwide Mut. Ins. Co., 8 N.Y.3d 283, 291-92, 864 N.E.2d 1272, 1277-78 (2007). ESI blurs our traditional notions of physical “care, custody and control” of information, which is the conventional standard for preservation, collection and production of information. When information is stored in “The Cloud,” with various parts on different servers around the world, what law applies, and how can the law of a single jurisdiction apply to such data? See M. James Daley, “Storm Clouds Gathering for Cross-Border Discovery and Data Privacy: Cloud Computing Meets the U.S.A. Patriot Act”, 13 Sedona Conf. J 235 (Fall 2012). What is the practical impact of this reality on companies that operate globally, especially companies in litigation or subject to investigations in various jurisdictions? As set forth below, there is a myriad of laws and issues to contend with from a global eDiscovery perspective.

Key Issues Concerning International eDiscovery Laws and Cross-Border Discovery

In our global marketplace, conflicting regulations and rules, and corresponding international disputes, concerning electronic disclosure of information in international litigation, arbitration and/or investigations are inevitable. There is a wide diversity of laws, rules, regulations and directives of various countries and regions regarding eDiscovery, eDisclosure, and data privacy and protection. See M. James Daley and Laura Clark Fey, “International Restrictions on Releasing Personal Information: What Steps
Although the electronic discovery reference model (EDRM; www.edrm.net) remains a helpful tool to visualize the process that surrounds the lifecycle of ESI in connection with meeting disclosure obligations, companies, and the advisors that serve them, entities also need to be aware of key issues concerning international eDiscovery legal requirements, including those discussed herein.

1. Data preservation and legal holds
   In the United States, it is well accepted that potentially relevant information must be preserved when litigation is either filed or is “reasonably foreseeable.” See Micron Tech., Inc. v. Rambus, Inc., 255 F.R.D. 135 (D. Del. 2009). In the United States, the information that is required to be preserved often is referred to as “subject to legal hold.” Before instituting a worldwide legal hold, however, it is important to consider whether the information subject to legal hold includes personal data, and, if so, where such personal data is located. Many countries have strict laws setting forth specific requirements for when personal data may be processed and transferred to another country.

   In the European Union and several other countries outside the United States, the mere issuance of a legal hold that impacts personal data can subject a company to data protection laws restricting the unauthorized “processing” of personal data. These laws usually broadly define “personal data” as any data which indentifies a person. Such laws typically define “processing” as any handling of the data that is outside the normal control and management by the individual data subject who is identified in, or identifiable through, the data. In this regard, a company mandate to take measures to even retain such data may, without a legitimate, independent basis for doing so, constitute an impermissible processing of personal information. See EU Data Protection Directive (95/46/EC).

   According to each country’s local laws and directives, the processing of personal data will likely be dependent upon the voluntary, informed consent of the data owner for a permissible purpose under that country’s laws—not the laws of the country where the disclosure may be required, such as the United States. Best practices suggest that the voluntary consent of data subjects to processing be obtained contemporaneous with issuance of a legal hold in these circumstances. If the data subjects are employees, however, it is important to keep in mind that in some jurisdictions, such as France, employees are deemed incapable of voluntary consent to processing of personal data for this purpose because they are considered to be in an unequal position vis-à-vis their employer. Also, consider that in some cases, the potentially relevant data may also be in the custody or control of a non-party person or company.

2. Data custodians, data controllers, data owners, data processors, and data subjects—knowing what they mean and how they impact eDiscovery
   Data custodians are the persons who are responsible for any data files, including email or other electronic communications. In the United States, when information needs to be collected from individuals, those individuals are generally referred to as “custodians.”

   A data controller is, under Article 2(d) of the European Union Data Protection Directive (the “Directive”), “the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data . . .” The Directive, which has been implemented to varying degrees by each of the European member states, requires that data
controllers adhere to certain principals when processing data. A summary of these principles can be found at this website maintained by the European Commission’s Directorate General for Justice:  http://ec.europa.eu/justice/data-protection/data-collection/obligations/index_en.htm.

Data ownership depends upon the laws of the jurisdiction in which the data is located. In the United States, contracts between companies and their employees and common employment law generally define the scope of such ownership. For an employee in the United States, there is no real expectation of privacy as it pertains to company-owned information. The company is typically deemed to be the owner of the data (e.g., work files and email) developed and used by an employee in connection with his or her employment by the company. Outside of the United States, the reverse is generally true: an employer is not deemed to “own” all information created by an employee, and an employee does have a reasonable expectation of privacy with respect to his or her work computer and electronic communications. Further, depending on the relevant laws, invading that privacy may constitute a criminal offense. Privacy rights are well-defined and developed fundamental rights in Europe.

A data processor is, under Article 2(e) of the Directive, “a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.” The data processor is different than the data controller, and generally processes data pursuant to the instructions or mandate provided to the data processor by the data controller.

Data subjects are identifiable persons to whom personal information relates. Typically such information indicates a person’s name, physical address, telephone number, email address, or physical, financial, economic, social or other cultural attributes of the individual that can be used to identify that individual.

3. Data privacy laws and blocking statutes
Several countries, including countries in Asia, South America and Europe, have data privacy and protection laws that prevent the transfer of data outside of such countries. These laws may also restrict the scope of data that may be transferred (i.e., data which is specifically responsive to a particular request). Data may need to be filtered in-country to remove personal or other sensitive information before it is transferred out-of-country assuming the data will continue to be processed out-of-country. Note, however, that current technology provides several options for, among other things, identifying, collecting, filtering and processing in-country and “behind the firewall” of a data controller. Consider whether the data will need to be reviewed locally before being transferred out-of-country, and what technology is available to assist in that process.

Conflicts can and do arise when there is a requirement to produce information in one country (such as the United States in connection with a litigation matter) and information that must be produced resides in another country where it is subject to data privacy and protection laws. Under authority by the U.S. Supreme Court in Société Nationale Industrielle Aérospatiale v. United States District Court for the Southern District of Iowa, 482 U.S. 522 (1987), U.S. courts with jurisdiction over a foreign litigant have authority to order the production of information outside the United States where such information would be subject to data restrictions in other countries. Of course, data protection authorities in countries outside of the United States do not view United States court decisions, even US Supreme Court decisions, as binding upon them.
Additionally, some countries have blocking statutes that are specifically designed to restrict or prohibit the disclosure of information for use in foreign proceedings even in the face of court-ordered disclosures. These statutes criminalize the exporting of information requested in foreign legal proceedings and create a conflict between compliance with the law of the jurisdiction that is requiring the disclosure and compliance with the law that is prohibiting such disclosure. Companies should therefore retain local counsel to advise regarding local laws and restrictions pertaining to blocking statues. Entities also should consider whether the Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (also known as the Hague Evidence Convention) presents a path by which evidence—note, not discovery—may be collected and provided. Unfortunately, this process is often lengthy and impractical, if it is even available as an option in a given country.

4. ESI collection

Before ESI can be collected, it has to be located. Key considerations include:

- Where is ESI stored?
- Who are the data owners, the data custodians and the data subjects?
- What are the countries where the ESI is located?
- How is the ESI stored (e.g., on what systems, servers, etc.)?
- Is any ESI on personal systems, such as personal email or personally owned devices?
- Is there cloud storage?
- Is it backed up?
- Where is it backed up?
- How often is it backed up?
- Are data backups encrypted, rotated, destroyed or overwritten?
- Is there a regular schedule pertaining to data backups?
- Who is in charge of the data backups?
- Are there any hard copy duplicates?

Before collecting ESI, choose an experienced data collection partner that is well-versed in collection requirements and considerations. These will include:

- jurisdictional requirements;
- chain of custody;
- whether consents will be required from the data subject before data can be collected and/or transferred, and the substance of those consents (informed, specific, written, etc.);
- whether the collector(s) will have to register locally in that country in connection with the work to be performed;
- providing expert testimony in court or any other tribunal to help explain and defend the collection process;
- ownership of the proper collection tools that will have the ability to collect different data codes (the collector should inquire about the various formats in which the data exists and the systems on which they exist); and
- in-country and out-of-country (or “remote”) data collections.

Also remember that in the United States, collecting data may require a “private investigator” state-issued license. In order for the evidence to be admissible in court, such license may have to be produced. Other states in the United States that do not require a private investigator license may still require other certifications and training to support the expertise of the forensic data collector in order for the collected evidence to be admissible in court.
Remote data collection poses some interesting legal issues. Because remote collection is so new, there are not many court decisions determining the applicability of data privacy laws to these situations. It seems reasonable, however, that the laws of the country from where the data is being collected should control the same as if the collection were performed in person at the data site (e.g., depending upon the applicable jurisdiction(s), providing notice, choice, obtaining informed consent, limiting collection (processing) to a specific purpose, maintaining integrity for onward transfers, access rights to data, etc.).

When data must be collected and forensically reviewed, and potentially transferred across country borders, certain legal issues and concerns must be considered, including the following:

- Do data protection laws applicable to the collection require the data collector to be physically present in-country?
- If so, how will equipment required in connection with the collection be transported into the country if that equipment is shipped from outside the country? Consider:
  - payment of tariffs;
  - declaration of equipment;
  - delays in customs if hardware is shipped; and
  - explaining the reasons for the in-country data collection visit, given client confidentiality concerns.

- How will the equipment used in connection with the transfer be transported out of the country?
  - Will the hardware be allowed on the airplane in a carry-on?
  - Should the hardware be checked? Will it be x-rayed and how will that affect the data and the equipment? Note that the client may not want hardware containing client data to be included in the collector’s checked baggage.
  - Will the hardware be shipped? Is the data encrypted and the package insured?
  - Some countries do not allow encryption of data that is being transported cross-border.

- Will the data collection will be performed in-person or remotely? In other words, whether the transfer of the collected data will be a physical transfer of a drive (or drives) or a technical transfer of data over the internet (a “remote collection”).

*Remote data collection* is where:

- the data collector sits in one country;
- the data collector connects to the data site, usually in another country, via a secure internet connection;
- an individual at the data site allows the data collector access to the computer device (note that consent is an issue of concern particularly if the data subject is not the individual granting access to the device and assisting with the collection process); and
the data collector is then able to collect data from that device which can be downloaded to a hard drive either at the data collector’s remote site or at the host data site itself (if data is downloaded to a device at the host data site, if necessary, the data on the device can be encrypted and shipped out of country for processing).

5. Multi-language components

Before collecting any data, inquire whether the data contains any multi-language components. It is more likely than not that it will. Ultimately, the data will need to be reviewed, so knowing the various languages—and identifying the primary and secondary languages—that will be contained in the data is essential to ensuring you have the personnel who are fluent in those languages involved in the review.

Other considerations include:

- Do you need any data to be translated? Or do systems for searching, collecting and reviewing data incorporate Unicode support?
- Do the various locations of the data implicate the potential for certain languages? Interview information technology and other personnel and data custodians for this information.
- Will you choose automated or human translation or a combination of both?
- Are there foreign languages that will need to be scanned via optical character recognition (OCR) software?
- Is the document review platform to be used capable of meeting your objectives on time and on budget, and can it handle the languages that will be included in your data set(s)? Can it search for various languages and identify them? Does your service provider have the ability to search and index all the multiple languages in one system? Does the service provider have experience in multi-language discovery?
- Take data samples, if possible, from key data custodians and search with language identification technology.

6. Transfer and Securitization of ESI

Once ESI has been collected, and assuming that it needs to be transferred across international borders, the legality of such transfer is subject to a number of legal issues and concerns. As mentioned above, consider whether the transfer implicates:

- any blocking statutes;
- data encryption requirements;
- customs requirements; and
- data privacy laws, such as those that would prohibit the transfer of personal data to a jurisdiction, such as the United States, where the data protection laws are not considered to be adequate as compared to the jurisdiction of the country from where the data is to be transferred.

Depending upon the jurisdictions involved in the transfer, check whether the transferee is in a country where the data protection laws are deemed to be inadequate by the country/jurisdiction of the transferor. If those laws are not adequate, then evaluate and execute appropriate registrations (such as the U.S. Safe Harbor Framework), documents and/or agreements to establish the proper
authority, procedures and controls to allow the transfer. These include data transfer agreements or other contractual clauses, model contracts, binding corporate rules and adequate technical and organizational measures to ensure the confidentiality, availability and integrity of the data.

Finally, remember the acronym “RED”. This stands for “redundancy, encryption and documentation.”

- **Redundancy**: *never, ever* take the original data or the only drive or device that such data is on. Make an exact copy of it, use that, and leave the original with the data controller/owner. One of the greatest risks involving the transfer of ESI is data loss.
- **Encryption**: *always* encrypt the data.
- **Documentation**: *always* have the appropriate documentation for the data collection and transfer. You will need it to get through customs to explain why you’re carrying encrypted data and to explain the purpose of the data transfer. Have a plan on how you’re going to get through customs *before* you get there.

### 7. The U.S. Patriot Act

The USA PATRIOT Act of 2001, which stands for United (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act of 2001, was enacted by the U.S. Congress in 2001 in order to expand the investigative ability of governmental agencies in the response to the terrorist attacks of September 11, 2001.

In May 2011, certain provisions of the Act were extended, including Section 215 (“Access to records and other items under the Foreign Intelligence Surveillance Act”), also known as the “library records” provision, which allows the government to petition a specially established FISA court to compel third parties to produce records so long as the information requested is relevant to protect against terrorism, among other things.

Recent news stories detailing information regarding U.S. surveillance under the purported “NSA Prism program” leaked by former National Security Agency (NSA) contractor Edward Snowden underscore the scope and reach of the Patriot Act. In essence, if the data resides in the U.S. or can be accessed by a person or entity with a U.S. presence, then the U.S. government has the ability to apply to the FISA court to access and copy that data, regardless of European Union data protection laws or the U.S. Safe Harbor program. Knowledge of such access as it pertains to the ultimate data owner may also be prevented pursuant to a gag order, injunction or a national security letter issued by a U.S. government agency.

The Patriot Act raises important considerations for entities involved in collecting data for purposes of eDiscovery. One key consideration is where the email or other data will be hosted. This is an important question to ask of any eDiscovery vendors, including, of course, vendors who will be hosting data in the “cloud.” Entities need to know where the servers hosting their data will be located. If the data is located in the U.S., then it will be subject to the Patriot Act. And if the data is hosted in the European Union, but the hosting company has a U.S. presence, then the data may likely be subject to the Patriot Act if the data can be accessed by that company which has a U.S. presence. The United States, however, is not the only jurisdiction that allows certain governmental access to cloud data: *See, infra, Daley, “Storm Clouds Gathering for Cross-Border Discovery and Data Privacy: Cloud Computing Meets the U.S.A. Patriot Act”, 13 Sedona Conf. J 235 (Fall*
8. The Sedona International Framework and Principles

In August 2008, The Sedona Conference® Working Group 6 (WG6) issued a public comment draft of “The Sedona Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and Discovery” (2008). This work represents the collective input of 123 members of WG6 from countries as diverse as Australia, Barbados, Brazil, Canada, China, England & Wales, France, Germany, Japan, Netherlands, Spain, Switzerland, Sweden, the United Kingdom and the United States, among others.

On February 11, 2009, the Article 29 Data Protection Working Party (the “WP”) issued its “Working Document 1/2009 on pre-trial discovery for cross border civil litigation” (also known as “WP158”). In WP158, the Working Party acknowledged the helpfulness of The Sedona Framework, noting that it sets out “relevant factors” U.S. courts should consider “when determining the scope of cross border discovery obligations.”

In December 2011, The Sedona Conference® WG6 issued a public comment version of its International Principles, entitled: “The Sedona Conference® International Principles on Discovery, Disclosure and Data Protection” (2012) which envision a three-stage approach to dealing with cross-border eDiscovery conflicts: (1) a stipulation or order from the U.S. court to extend special protections to data covered by data protection laws; (2) a scheduling order that phases discovery to permit time to implement data protection processes and to determine whether the same or substantially similar information is available from non-protected sources; and, (3) implementation of a legitimization plan to maximize simultaneous compliance with the foreign data protection law and the U.S. discovery obligation. The theory is that parties and the court will find that some or all of these steps may avoid or minimize the conflict that might otherwise arise.

The Sedona International Principles include six Principles, each with a comment section to elucidate its purpose and supporting authorities (e.g., treaties, case law and other authorities). The six Sedona International Principles on Disclosure and Data Protection are:

1. With regard to data that is subject to preservation, disclosure, or discovery, courts and parties should demonstrate due respect to the Data Protection Laws of any foreign sovereign and the interests of any person who is subject to or benefits from such laws.
2. Where full compliance with both Data Protection Laws and preservation, disclosure and discovery obligations presents a conflict, a party’s conduct should be judged by a court or data protection authority under a standard of good faith and reasonableness.
3. Preservation or discovery of Protected Data should be limited in scope to that which is relevant and necessary to support a claim or defense in order to minimize conflicts of law and impact on the Data Subject.
4. Where a conflict exists between Data Protection Laws and preservation, disclosure or discovery obligations, a stipulation or court order should be employed to protect Protected Data and minimize the conflict.
5. A Data Controller subject to preservation, disclosure or discovery obligations should be prepared to demonstrate that data protection
obligations have been addressed and that appropriate data protection safeguards have been instituted.

6. Data Controllers should retain Protected Data only as long as necessary to satisfy legal or business needs. While a legal action is pending or remains reasonably anticipated, Data Controllers should preserve relevant information, including relevant Protected Data, with appropriate data safeguards.

9. The Proposed New EU Data Protection Regulation

On January 25, 2012, the European Commission adopted a proposed EU Regulation, with the ambitious goal of reforming the EU’s legal framework for data protection. It has been characterized by one leading expert as a revolution in European data protection law of “Copernican” proportion.

The objectives of the proposed EU Data Protection Regulation include providing for greater uniformity of data protection efforts among EU member states, as well as centralization of authority (“one stop shop”) for data protection issues for multinational corporations. The key provisions of the draft EU Regulation adopted by the EU Commission include:

- A single Data Protection Authority for Multinationals;
- Significant Restriction of Employee Consent for Data Processing;
- Elimination of Current Processing Notification Requirements;
- Data Protection Officer if More than 250 Global Employees;
- “Right to be forgotten” and “Privacy by Design” Requirements;
- Notification of Data Security Breaches to Regulators and Persons;
- Simplified Procedures for Transferring Personal Data Outside EU;
- Increased Independence and Power for Data Protection Authorities; and
- Data Protection Violation Fines: up to 2% of a company’s global annual turnover (e.g., annual worldwide gross sales revenue).

International in-house counsel can take several practical steps to prepare for these objectives and tentative requirements. Such steps include:

- Let your corporate voice be heard—provide input to the EU Commission and EU Parliament;
- Identify and prepare a Data Protection Officer;
- Develop compliant policy and procedure framework;
- Conduct a data protection and privacy assessment;
- Understand and repair data protection vulnerabilities;
- Integrate data protection into associate training;
- Understand the proposed new obligations on data processors; and
- Take a fresh look at Binding Corporate Rules, as a means to comply with the spirit and letter of many of the new provisions.

A number of Member States—including the UK, Germany, Sweden and Belgium—have said that the proposed rules are too prescriptive, and have argued for certain provisions of the draft to be removed entirely. The regulation is currently being “fast tracked” through the European Parliament under the direction of the main EU Parliament rapporteur, Jan Philipp Albrecht, German Green Party Member of the European Parliament (MEP). On January 8, 2013, Albrecht issued a draft report (the “Albrecht Report”) on the proposed regulation to the EU Parliament’s Committee on Civil Liberties, Justice and Home Affairs (“LIBE” Committee) that posed serious questions regarding the formulation and impact of the proposed regulation. The Albrecht report, over 215 pages in length,
proposes over 350 draft amendments to the proposed regulation, and is certainly not the last word in the EU legislative process. Some of the key amendments proposed include:

- Broadening the notation of “personal data” to include internet protocol (IP) addresses, cookies and other unique electronic identifiers that leave traces that can be used to identify specific natural persons;
- Recognizing a new category of “pseudonymous” data that would qualify for lighter treatment under the regulation, and exempting truly anonymous data from the regulation altogether;
- Introducing a new role of “Data Producer” for entities that create automated data processing or filing systems, which will need to comply with privacy by design and privacy by default principles;
- Extending the time, from 24 to 72 hours, for reporting data breaches to data protection authorities (DPAs), and restricting this duty to situations where the breach is likely to adversely affect the protection of personal data or privacy;
- Establishing specific, informed consent by data subjects as the cornerstone of the new data protection framework—that is, “if you want my data, ask for consent;”
- Limiting the ability of data controllers to rely on protecting their legitimate interests as a legal basis for unilateral processing of personal data;
- Expanding rights of access and retrieval of one’s personal data;
- Limiting the scope of the proposed “right to be forgotten,” where someone has specifically agreed to make his/her personal data public;
- Strengthening the right to object to processing of one’s personal data;
- Expanding privacy notice obligations, and extending them to joint data controllers;
- Providing for effective legal redress before courts or DPAs for regulation violations;
- Restricting the scope and manner of use of personal data for behavioral profiling;
- Requiring the role of Data Protection Officer (DPO) for entities that impact the personal data of more than 500 persons, either internally or externally;
- Requiring Data Protection Impact assessments;
- Mandating data protection by design and default requirements for systems that process personal data;
- Increasing the burden on the private sector for approval of international data transfers;
- Empowering Data Protection Authorities to impose strong fines on companies that violate EU data protection rules; and
- Establishing a tiered system for sanctions and fines, but making the highest level of fine (up to 2% of annual gross global income) apply by default, unless a lower category of fine is established for an infraction.

The immediate next steps in the EU Parliamentary process include an upcoming presentation in the fall of 2013 to the EU Parliament in plenary session.
10. Data Loss Prevention (DLP) Systems

Another eDiscovery issue of note for in-house counsel relates to the impact of data loss prevention (DLP) systems. As data breaches proliferate in frequency and severity, companies are increasingly turning to Data Loss Prevention (“DLP”) systems to monitor and prevent unauthorized use and transmission of confidential information, as well as to increase compliance with regulatory requirements (e.g., FCPA, insider trading, proper handling of personal data and non-discrimination). The market for content-aware DLP systems is growing at a rate of over 20% per year, according to industry experts. And with the increased data privacy and security challenges posed by the explosion of social networking, and other emerging technologies, this trend is likely to continue.

Although DLP systems help organizations safeguard strategic information and enhance compliance, they can create a number of unintended eDiscovery risks and costs if they are not carefully configured and maintained. For example, DLP systems, though not intended as general data archival systems, may actually store information that can be relevant to pending or reasonably foreseeable litigation or regulatory actions, thereby triggering a legal duty of preservation. Given the significant sanctions that courts have levied for general violations of the preservation duty, all pertinent parts of an organization (IT, Legal, Security, etc.) need to know and weigh these risks and costs when considering deployment of a DLP system. See Daley and Fey, “Exploring Data Loss Prevention Systems for Legal Hold and E-Discovery,” ARMA International Information Management (Sept/Oct 2012).

11. Technology-Assisted Review

Technology-assisted review (“TAR”) is also referred to as “predictive-coding” review or “computer-assisted” review. TAR can be summarized as follows: using technology, senior lawyers select a few thousand documents from a larger data set, analyze them for relevancy and privilege, and upload that analysis to artificial intelligence, which then creates one or more algorithms. Those algorithms replicate the attorney analysis technologically and apply it to the remainder of the ESI in an iterative process. As a result, the costs of a manual review are substantially lessened.

TAR is designed to replace search terms because search terms can be inaccurate. Search terms produce a high amount of false positives, whereas TAR can analyze a data set faster and more precisely than by utilizing search terms.

The steps of TAR are as follows:

1. A representative sample of a data set of electronic documents is established. Most commonly, random sampling of the full set of data is used. This is called a “seed set.” Search terms can be used to help create the seed set, but they should be used sparingly.
2. An attorney or a team of attorneys who are knowledgeable in the subject matter review the seed set and determine which documents are responsive (referred to as “initial coding”). Based upon this initial coding, the TAR tool will begin to “learn” how to score documents for relevance.
3. TAR will use this knowledge to develop a new smaller set of documents for a senior attorney to review for responsiveness. The results from this review will be loaded into the TAR tool to allow it to continue perfecting its algorithm(s).
4. The TAR tool will continue providing additional sets of documents to the attorney to review until the tool has completed the creation of its algorithm(s). Through this learning process, the reviewing attorney will “train” the algorithm(s) by evaluating where the attorney’s decisions differ from those of the computer and making
appropriate adjustments. This process will be repeated until the attorney is satisfied
the TAR tool is identifying responsive documents effectively and efficiently.
5. TAR then prioritizes the remainder of the documents most likely to be relevant to
the attorney reviewer. The eDiscovery service provider and eDiscovery counsel
(including any company in-house counsel) will implement a process that will often
include a level of “quality control” attorney review before responsive documents are
produced in the matter.

By using TAR, a linear or human responsiveness review can be eliminated entirely if the
comfort level and sensitivities of the review allow it. For additional information on TAR,
see EDRM’s Computer Assisted Review Reference Model, which is a useful reference
tool for e-discovery practitioners venturing into TAR.

One of the primary benefits of TAR is the prioritization of the documents in the data set.
Highest scores are placed on documents deemed most likely to be responsive. Because
TAR can provide the attorney reviewers a “confidence score” of the responsiveness of
each document: (i) the process is more transparent than a traditional document review;
and (ii) the turnaround time is faster than by utilizing only a search term review. TAR can
also be used to assist in classifying potentially privileged documents with a fairly high
degree of recall.

The following are two case scenarios involving TAR:
24 2012), the court approved the use of predictive coding especially with respect to
matters involving large volumes of data, noting the efficiencies that can be achieved
by using TAR and that “the Federal Rules of Civil Procedure do not require
perfection.” In that case, Judge Peck emphasized that collaboration is critical when
it comes to using TAR. The two sides must get together early in the case and agree
on how it will be used. This decision created a major upswing in the U.S. in the use
of TAR.

B. Company X, a defendant in litigation, used a combination of electronic search
functions to identify relevant documents. Keyword culling was used first, reducing
the complete set of collected documents from approximately 20 million to 4 million.
Duplicates were then removed from the data set, resulting in approximately 2.5
million documents remaining. A subset of documents was then selected randomly
from the set of approximately 2.5 million documents (the “subset”). Statistical
sampling tests were applied to the subset. As a result, Company X obtained two
projections, each with a 99% confidence rate that: (1) between .55 and 1.33 percent
of the 2.5 million documents not in the subset would be responsive; and (2) between
1.37 and 2.47 percent of the original approximately 20 million documents were
responsive. TAR was able to reduce the likelihood of responsive documents
substantially as opposed to Company X’s “manual” keyword search on the set of 20
million documents, which had identified as much as 16% of the original 20 million
as potentially responsive.

Company X determined to use TAR to identify relevant documents to be produced
from the set of approximately 2.5 million documents. The plaintiffs, however,
requested that Company X employ predictive coding on its original set of
approximately 20 million documents. The court determined that Company X’s
procedure satisfied its eDiscovery obligations, on the basis that the costs associated
with the process requested by the plaintiffs would have been substantial and would
not have produced a more beneficial and responsive set of documents.
In the United States, TAR is becoming more of an accepted method of identifying responsive documents. Interestingly, the United Kingdom and the rest of the European Union may be more likely to use and accept TAR than the United States because of the larger acceptance of cost/proportionality arguments outside the United States.

TAR can be a useful tool not only for analyzing large data sets but for dealing with cross-border eDiscovery issues. For example, TAR can be utilized in-country to identify personal information or other sensitive information that should not leave country borders for out-of-country processing including review.

*The Forecast for International In-House Counsel*

Certainly, there is stormy digital weather ahead for international in-house counsel tasked with managing the legal risk and cost of cross-border e-discovery. Every stage of the EDRM model presents unique and additional legal and practical challenges. These range from additional legal data privacy, data protection and blocking statute considerations, to questions of jurisdiction and sovereignty. Even the “locus” of ESI is difficult to determine, leaving companies without a predictable legal framework for assessing legal risk.

In this climate, awareness of the above issues is the most important first step in managing related risk and cost. International corporate counsel should consider seeking the guidance of a trusted advisor that understands both the pertinent technology and procedural and substantive law. This includes how notions of jurisprudence, privacy, data protection and discovery conceptually differ among the various jurisdictions, as well as how they, as a practical matter, apply to the specific ESI data, containers and systems involved. In time, with sustained effort and resources such as those of The Sedona Conference® and others, the forecast should improve, with clearer guidance and practical, cost-effective international e-discovery protocols and standards.

***

**Jayne Rothman** is Vice President, Corporate Counsel for Epiq Systems, Inc. and its subsidiary companies. At Epiq, Jayne manages general matters including corporate, mergers & acquisitions, commercial transactions, litigation, employment, data privacy, compliance, risk management, insurance, intellectual property, and management of outside counsel, among others.

Prior to joining Epiq in 2005, Ms. Rothman practiced at Dewey LeBoeuf LLP in Los Angeles, where she represented ABC/ESPN and creditors in the Worldcom and United Air Lines Chapter 11 cases, and at Weil Gotshal & Manges LLP in New York, representing corporate M&A and restructuring clients including Enron Corp., Hughes Electronics Corp., Old Mutual Plc and Six Flags, Inc. Ms. Rothman also clerked for two years for Chief Judge Mark W. Vaughn, U.S. Bankruptcy Court, D. N.H. Jayne Rothman can be contacted via e-mail at jrothman@epiqsystems.com or phone at (913) 621-9950.

**Alison Wisniewski** is Senior Legal Counsel for Epiq Systems, Inc. and its subsidiary companies. At Epiq, Ms. Wisniewski works on general corporate matters including sales transactions, commercial transactions, mergers & acquisitions, data privacy, compliance, risk management, intellectual property, and transactional employment matters, among other things.

Prior to joining Epiq in 2010, Ms. Wisniewski practiced in house at an asset management company called Crown Northcorp in White Plains, NY, where she assisted the FDIC in the dissolution of various banks throughout the country. Ms. Wisniewski has also
practiced at Kramer Levin Naftalis & Frankel LLP and Sidley Austin LLP, each in New York, NY, representing corporate and private equity clients in various matters including mergers & acquisitions, securities filings and corporate governance.

Alison Wisniewski can be contacted via e-mail at awisniewski@epiqsystems.com or phone at (212) 225-9267.

M. James “Jim” Daley, Esq., CIPP/US is co-founder of Daley & Fey LLP, a boutique law firm devoted to helping clients reduce legal risk, contain cost, and ensure compliance with records management, electronic discovery and data privacy obligations. Jim serves as a trusted advisor for a wide variety of Fortune 500 clients, as was profiled in 2010 by The American Lawyer as “Who You ‘Gonna Call” for national coordinating e-discovery counsel. Jim is also frequently selected as an Independent Expert by courts, clients and other counsel to evaluate corporate e-discovery, records management and data privacy conduct.

Jim leverages over 30 years of complex litigation experience, his Master’s Degree in Information Systems, and his experiences as Co-Chair of The Sedona Conference® Working Group Six on International Electronic Information Management, Discovery and Disclosure (2005-2012) to help U.S. and multi-national clients develop practical, cost-effective solutions to records and information management, e-discovery, and data privacy compliance challenges. Jim and his team help clients develop and implement process and technology solutions including: data privacy and security controls; disposition of legacy electronic media and print information; e-mail archiving and electronic records management solutions; legal hold management and compliance monitoring solutions; RIM policy and procedure; RIM and legal hold training; U.S. and global records retention schedules; selection of preferred vendor panels; and litigation and regulatory compliance readiness programs, among others. Jim also helps global companies successfully navigate the risk and costs of cross-border transfers of data in business, legal and regulatory contexts, as well as cloud computing, social networking and other emerging technologies.


M. James Daley can be contacted via e-mail at jdaley@daleylegal.com, via post at 5750 W. 95th St., Suite 310, Overland Park, KS  66221 USA, or via phone at (913) 948-6302 (Office) or (913) 522-8901 (Mobile).

Laura Clark Fey is co-founder of Daley & Fey LLP. Laura, a Certified Information Privacy Professional (CIPP/US), assists U.S. and multinational corporations in developing and implementing practical, legally compliant solutions to their specific challenges at the crossroads of law and information technology. Laura utilizes her experience and expertise in U.S. and international data privacy and protection; e-discovery and legal holds; ethics; and regulatory retention requirements to help clients
develop policies, processes and programs designed to address their unique needs based upon their regulatory and litigation profile, as well as their corporate culture, risk tolerance and budget.

In her specialized law and technology practice, Laura draws upon over twenty years of litigation and trial experience successfully defending U.S. and multinational corporations in a variety of complex matters—including attorney general actions, multi-district litigation, class actions, and consolidated and individual cases—in state and federal courts throughout the country. Prior to founding Daley & Fey with M. James Daley, Laura was an equity partner in an Am Law 100 firm and a trial attorney with the U.S. Department of Justice. During her time with the Department of Justice, Laura was a recipient of the Department’s Outstanding Performance Award.

Laura has been selected as a Super Lawyer® for six straight years. Super Lawyers® identifies the top five percent of lawyers in each state (e.g., Missouri and Kansas) as chosen by their peers and through independent research by Law & Politics. Laura has been named to the publication’s list of “Top 50 Women” practicing in Missouri and Kansas. Laura also has been named a Top Attorney in Business Services by Super Lawyers® Corporate Counsel Edition.

Laura Clark Fey can be contacted via e-mail at lfey@daleylegal.com, or via phone at (913) 948-6301 (Office) or (816) 518-6554 (Mobile).

Epiq Systems is a leading global provider of technology-enabled solutions for electronic discovery, bankruptcy and class action administration. We offer full-service capabilities to support litigation, investigations, financial transactions, regulatory compliance and other legal matters. Our innovative technology and services, combined with deep subject-matter expertise, provide reliable solutions for the professionals we serve.

Daley & Fey LLP is a boutique law firm with specialized expertise in the areas of e-discovery, data protection and privacy, records governance, information technology and data security. Daley & Fey’s lawyers and analysts are dedicated to helping organizations reduce legal risk and cost and enhance compliance with information laws and regulations, including data protection and privacy regulations, regulations governing records retention, and rules and laws governing e-discovery. Daley & Fey’s lawyers and technologists assist U.S. and multi-national corporations in a wide variety of industries, including but not limited to healthcare, insurance, media, manufacturing, retail, food & beverage, pharmaceutical and medical device, travel, technology and financial services, in developing reasonable, right-sized solutions to a multitude of U.S. and international records governance, e-discovery and data privacy challenges.