Computer Law Review International

CRi

Sonderdruck

A Journal of Information Law and Technology

Karl Geercken · Kelly Holden · Michael Rath
Mark Surguy · Tracey Stretton

Cross Border E-Discovery

How to manage potential evidence in an international environment

Verlag Dr. Otto Schmidt Köln

www.cr-international.com

Imprint CRi

Editor: RA Ulrich Gasper, LL.M. (Edinburgh) · Adriane Braun (editorial assistant) · Address: Gustav-Heinemann-Ufer 58 · D-50968 Cologne · Phone +49-2 21-9 37 38-180 · Fax +49-2 21-9 37 38-903 e-mail: cr-international@otto-schmidt.de

Publishing House: Verlag Dr. Otto Schmidt Gustav-Heinemann-Ufer 58 · D-50968 Cologne Phone +49-2 21-9 37 38-01 · Fax +49-2 21-9 37 38-943 · e-mail: verlag@otto-schmidt.de

Schedule for Publication: The issues are published on the 15th of February, April, June, August, October and December.

Production: Print-Set: Fotosatz Pfeifer, Lochhamer Schlag 11, 82166 Gräfelfing · Print: Boyens Offset GmbH & Co. KG, Wulf-Isebrand-Platz 1–3, 25746 Heide

Advertisements: Responsible for advertisements is Ralf Pötzsch from whom a list of current prices can be obtained. Phone +49-2 11-8 87-1490 · Fax +49-2 11-8 87-1500 · e-mail: fz.rws@fachverlag.de

Subscription rates: (Outwith the subscription to the journal COMPUTER UND RECHT) 189,- € per annum (for members of the Deutsche Gesellschaft für Recht und Informatik e. V. 169,- € per annum). Single copies cost 34,80 €. All prices exclude postage and include statutory VAT. Subscriptions are billed annually at the beginning of the subscription period for the current calendar year (pro rata).
COMPUTER LAW REVIEW INTERNATIONAL is free for subscribers to the journal COMPUTER UND RECHT.

Subscription: At any book shop or at the publishing house.

Cancellation: Must be made six weeks before the end of the year.

ISSN 1610-7608

CRi

Articles

Karl Geercken/Kelly Holden/Michael Rath/Mark Surguy/Tracey Stretton

Cross Border E-Discovery

How to manage potential evidence in an international environment

In the context of internal or regulatory investigations or other legal proceedings, companies located in Europe may be forced to disclose electronically stored information such as e-mails on short notice in order to comply with any such internal or regulatory request or applicable procedural electronic discovery regulations. These disclosure requirements may have considerable breadth, and non-compliance can lead to severe sanctions.
Part I of this article describes the American procedure of e-discovery. Part II provides a brief description of the British concept of e-disclosure and considers how it differs from the American concepts of e-discovery. Part III shows – as one prominent example for civil code jurisdictions in the European Union (for an overview of other jurisdictions see The Sedona Conference, International Overview of Discovery, Data Privacy and Disclosure Requirements, September 2009) – the German regime for e-discovery requests and highlights some data protection issues to be observed. Part IV examines how the conflict existing between the common law concept of e-evidence and the civil law principles could be harmonized. Finally, part V gives some examples of how technology can be used to support e-discovery and to establish processes in compliance with applicable data privacy laws.

I. The American Procedure of E-Discovery

Unlike in many civil law countries, the process of "pre-trial-discovery" is an important, costly, and timely part of the American legal system. It is at this pre-trial discovery stage that issues relating to e-discovery arise. The purpose of this judicial preliminary process is the finding of facts and/or discovery of the relevant evidence and is, to a large extent, conducted by the parties without the participation of judges. During this process, the parties can demand from their adversaries the presentation of comprehensive information concerning all facts and evidence which could be "relevant" to the alleged claim or defense, according to Rule 26 of the Federal Rules of Civil Procedure ("FRCP").[1] The definition of "relevant" is broad; evidence may be considered relevant, for example, if it can *lead* to the discovery of admissible evidence.[2] Extensive and detailed pleadings are generally not necessary under U.S. notice pleading rules, in part because of the liberal and expansive pre-trial-discovery tools that are available to U.S. litigants and allow them to identify relevant facts and witnesses. In practice, requests for information are carried out by written interrogatories (i.e. written questions to the opposite party), judicial discovery orders, or requests for the production of documents or things (i.e. a request brought forward to a litigant by another party's lawyer to prepare and present relevant documents). Significantly, according to Rule 34 of the FRCP, it is clear that electronically stored information ("ESI") is governed by pre-trial-discovery regulations in the same manner as documentary evidence.[3] This means that a company's electronic information system (its servers, hard drives, back up systems, software document management systems and third party document retention systems) is also subject to discovery.[4]

1. Documents Subject to E-Discovery According to the FRCP

Similar to the expansive interpretation of the term "relevant", the term "documents" is likewise broadly defined under U.S. law. According to Rule 34(a) of the FRCP, ESI not only includes mere text but also includes "writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations."[5] Furthermore, the final versions of the aforementioned documents are covered by e-discovery rules along with drafts, versions of the document drafted by various editors, annotations and notes. In the absence of a contrary agreement between parties, metadata (which is data on the documents themselves, such as the name of the editor and the date of creation and amendments of the document) may also be subject to disclosure.

2. Duty to Preserve

As part of the e-discovery requirements, companies have an obligation to collect and store electronic data in a secured manner, which is otherwise known as the "duty

▷ Karl Geercken and Kelly Holden are attorneys at Alston & Bird LLP, New York, Dr. Michael Rath is attorney, certified expert lawyer on information technology and partner at Luther, Cologne, Germany, Mark Surguy is solicitor and legal director at Pinsent Masons, London, U.K., and Tracey Stretton works as legal consultant with Kroll Ontrack, London, U.K. Further information about the authors at p. 96.

1 *See* Fed. R. Civ. P. 26(b)(6)(1) ("Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any non privileged matter that is relevant to any party's claim or defense including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter.")

2 *See* Fed. R. Civ. P. 26(b)(1) ("Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.")

3 *See* Fed. R. Civ. P. 34, *Producing Documents, Electronically Stored Information, and Tangible Things, or Entering onto Land, for Inspection and Other Purposes*.

4 For example, a party to a lawsuit may rightfully request access to an opponent's e-mails relating to a certain time period or for documents containing certain key words. *See Froemming/Rosenthal*, CRi 2007, 69 et seq; *Coleman Holdings, Inc. v. Morgan Stanley*, No. 502003CA00 5045XXOCAI, 2005 WL 679071, at *1 (Fla. Cir. Ct. Mar. 1, 2005).

5 *See* Fed. R. Civ. P. 34(a).

to preserve." One important question is *when* a company's duty to preserve is triggered. In the U.S., the *Zubulake* decisions – a series of five opinions stemming from an otherwise routine employment discrimination dispute – are considered to be landmark e-discovery cases.[6] The opinions provide valuable guidance for parties and their counsel as to preserving and producing electronic discovery materials.

In *Zubulake V*, the Southern District of New York clearly established that counsel have a duty to communicate to their clients the discovery obligations so that all relevant information can be uncovered and retained. In answering the question as to when this obligation begins, the court stated that such "duty to preserve" attaches "when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation."[7] In other words, the duty is triggered when litigation is reasonably anticipated.[8] The duty to preserve applies to both plaintiffs and defendants and a plaintiff's duty is often triggered far before the litigation is commenced.[9] Unlike a defendant, a plaintiff has control over the commencement of the litigation and typically has greater advance notice of the litigation.[10] At that point, the counsel and the company have a duty to retain all relevant documents in existence or created thereafter.[11]

Evidence can often be lost within companies that use information "back-up" programs, which automatically retain and then discard documents after set periods of time. For example, it is not uncommon for an American company to have a Document Retention Plan ("DRP") in place as part of company policy. A typical DRP may include automatic document retention and destruction schedules. Accordingly, in order to limit the potentially serious consequences of unintentional destruction or loss of evidence, Rule 37(e) of the FRCP stipulates that no procedural sanction may be imposed against a party if the loss of data was caused as a result of a "routine, good-faith operation of an electronic information system."[12] This rule is often referred to as the "Safe Harbor" rule and is discussed in further detail later in this article.

3. Litigation Hold

Once the duty to preserve attaches, counsel must identify and speak directly with all relevant employees, as well as the client's information technology department, in an effort to preserve documents and information pertinent to the anticipated litigation.[13] A primary method of adhering to the duty to preserve involves issuing an initial and possibly subsequent "litigation holds," which are notices distributed to company employees in an effort to prevent the destruction of any potential evidence. The litigation hold is "only the beginning" of proper discovery obligations, however, and counsel must oversee compliance with the litigation hold and monitor their clients' efforts to retain and produce relevant documents.[14] As discussed further in the sanctions section below, a counsel's failure to follow through with assuring compliance with litigation holds or discovery obligations can lead to severe repercussions.[15]

4. Levels of Culpability for Violations of Discovery Obligations

In January 2010, the U.S. District Court for the Southern District of New York issued an opinion, entitled "*Zubulake* Revisited: Six Years Later" that addressed the previous *Zubulake* decisions and outlined culpability standards for various violations of discovery obligations.[16] In this case, the issue of e-discovery violations was triggered when defendants noticed gaps in plaintiffs' discovery productions. In short, multiple plaintiffs "failed to timely institute written litigation holds and engaged in careless and indifferent collection efforts after the duty to preserve arose," which resulted in some documents likely being lost or destroyed.[17]

The judge reviewed and defined three levels of culpability in the context of ESI – negligence, gross negligence, and willfulness – as follows: (1) negligence is conduct which falls below the standard established by law for the protection of others against unreasonable risk of harm, it may arise where the negligent party is unaware of the results that may follow its (in)actions and it may also arise when the party has considered possible consequences and exercised its own judgment; (2) gross negligence is ordinary negligence to a greater degree; and (3) willfulness is conduct that is intentionally done in disregard of a known or obvious risk that was so great as to make it highly probable that harm would follow.[18]

The judge then applied these definitions to particular conduct in the context of ESI discovery. The following conclusions made by the judge offer guidance on the culpability that attaches to various levels of unacceptable conduct:

6 The *Zubulake* decisions consist of a series of five opinions. Laura Zubulake, the plaintiff, sued her former employer under federal, state, and city law for gender discrimination and illegal retaliation. She moved to compel defendant to produce e-mails that existed only on back up tapes. After years of discovery disputes between the parties, this suit led to a detailed series of discovery-related opinions and became a leading case for discovery guidelines. The fifth and final opinion, *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422 (S.D.N.Y. 2004) (hereinafter "*Zubulake V*"), and the fourth opinion, *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003) (hereinafter "*Zubulake IV*"), in particular, detail the obligations of counsel and clients to preserve electronically stored information. As regards early case law under the amended Rule 34 of the FRCP *see Froemming/Rosenthal*, CRi 2007, 69 et seq.

7 Although *Zubulake* filed her initial charge of gender discrimination in August 2001, the court held that the duty to preserve attached as early as April 2001, because litigation was "reasonably anticipated" at that time. *See Zubulake IV*, 220 F.R.D. at 216-17 (internal citations omitted).

8 *Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC*, No. 05 Civ. 9016 (SAS), 2010 U.S. Dist. LEXIS 1839, at *14 (S.D.N.Y. Jan. 11, 2010) ("It is well established that the duty to preserve evidence arises when a party reasonably anticipates litigation.") (internal citations omitted).

9 *See id.* (citing *Innis Arden Golf Club v. Pitney Bowes, Inc.*, 247 F.R.D. 335, 340 (D. Conn. 2009), which found that the duty to preserve arises when a plaintiff retains counsel for a potential action but has not yet identified possible defendants).

10 *Id.* at *14.

11 *See Zubulake IV*, 220 F.R.D. at 218.

12 Fed. R. Civ. P. 37(e).

13 *See Zubulake V*, 229 F.R.D. at 439.

14 *See id.* at 432.

15 For example, in *Coleman Holdings, Inc. v. Morgan Stanley*, the court imposed significant sanctions on counsel for its failure to locate and timely produce backup tapes in response to plaintiff's discovery requests, finding that such behavior "severely hindered [plaintiff's] ability to proceed." *Coleman Holdings, Inc.*, 2005 WL 679071, at *6.

16 *Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC*, No. 05 Civ. 9016 (SAS), 2010 U.S. Dist. LEXIS 1839 (S.D.N.Y. Jan. 11, 2010) (hereinafter, "*Zubulake* Revisited"). This case is also of particular interest because it looks at preservation and spoliation of ESI from the plaintiff's perspective.

17 *Id.* at *6.

18 *See id.* at *7-10.

- failure to obtain records from non-key players (negligence)[19]
- failure to preserve evidence resulting in the loss or destruction of relevant information (negligence, at a minimum)
- failure to issue a written litigation hold (gross negligence)
- failure to collect records from key players and ensure their electronic records are preserved (gross negligence or willfulness)
- intentional destruction of relevant records after duty to preserve has attached (willfulness)

The determination of what level of culpability certain conduct creates is fact-specific and made on a case-by-case basis. The above examples and the *Zubulake* Revisited opinion generally, however, offer the most recent analysis and review of discovery obligations in the ESI context.

5. Sanctions for Infringement of Discovery Obligations

Discovery violations are not taken lightly and American courts are not shy in imposing significant sanctions in the event of a violation. Under the Doctrine of Spoliation, the breach of a discovery order can lead to considerable sanctions for the company involved in the proceedings.[20] Possible sanctions may include striking pleadings, taking certain matters as proven, holding a party in contempt, preventing the party in breach from relying on its evidence on a specific issue (which could have the effect of reversing the initial burden of proof), permitting use of an adverse inference instruction to the jury, or, ultimately, dismissal.[21] Additionally, and commonly, the party in breach may be ordered to pay considerable fines.

In the *Zubulake* case, defendant's counsel dutifully advised their clients of their discovery obligations regarding plaintiff's looming lawsuit. The court even noted that defendant's counsel "came very close to taking the necessary precautions".[22] But, because the court held that the defendant had willfully destroyed possibly relevant information, the court awarded sanctions to plaintiff. Specifically, plaintiff received not only the costs of both additional re-depositions and the motion to compel, including attorneys' fees, but plaintiff was also awarded an adverse inference jury instruction with regard to deleted or lost e-mails.[23]

Although the defendants acted willfully in the *Zubulake* case, intentional behavior is not always required in order for sanctions to apply.[24] As discussed above, the *Zubulake* Revisited opinion outlines the various levels of culpability, including ordinary negligence, that can trigger sanctions. Additionally, in 2002, the Second Circuit noted that courts have broad discretion in determining sanctions and held that "discovery sanctions, including an adverse inference instruction, may be imposed where a party has breached a discovery obligation not only through bad faith or gross negligence, but also through ordinary negligence."[25]

A recent series of opinions by the U.S. District Court for the Southern District of California serve as a cautionary tale that discovery violations can lead to hefty sanctions in the U.S. In *Qualcomm Inc. v. Broadcom Corp.*, the trial judge sanctioned Qualcomm and its outside counsel, and ordered Qualcomm to pay defendant's $8.5 million attorney fees, for intentionally or recklessly withholding "tens of thousands of e-mails" after submitting declarations stating that no such documentary evidence existed.[26] Fortunately for the attorneys, a later opinion in the *Qualcomm* series vacated the sanctions and found that although there was no doubt that the "massive discovery failure resulted from significant mistakes, oversights, and miscommunication on the part of both outside counsel and Qualcomm employees," because the outside counsel also made significant efforts to comply with their discovery obligations and the employees of Qualcomm deliberately misled the attorneys, such attorneys would not be sanctioned.[27]

As evidenced by the *Qualcomm* case, producing some, but not all, of ESI material may be a faulty step that leads to sanctions on parties and/or attorneys. In *Coleman Holdings, Inc. v. Morgan Stanley*, Coleman sought access to the e-mails of those Morgan Stanley employees involved in the transaction in dispute from a certain time period as well as those e-mails containing certain search words.[28] Although Morgan Stanley timely produced some of its employees' e-mails, more than a thousand additional back up tapes (which included an additional

19 *See id.* at *12-13, 31.

20 Spoliation is "destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation." *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir. 1999). *See also Zubulake* Revisited, 2010 U.S. Dist. LEXIS 1839, at *14 (noting that the spoliation of evidence "may result in the imposition of sanctions by a court because the court has the obligation to ensure that the judicial process is not abused").

21 Fed. R. Civ. P. 37, *Failure to make Disclosures or to Cooperate in Discovery Sanctions. See also Zubulake* Revisited, 2010 U.S. Dist. LEXIS 1839, at *24 (noting that a court should always impose the least harsh sanction that can still provide an adequate remedy, and noting that possible sanctions "from least harsh to most harsh" include: "further discovery, cost-shifting, fines, special jury instructions, preclusion, and the entry of default judgment or dismissal") (internal citations omitted). For a sample of special jury instructions, *see Zubulake* Revisited, 2010 U.S. Dist. LEXIS 1839, at *104.

22 *Zubulake V*, 229 F.R.D. at 435.

23 *Id.* at 439.

24 *See, e.g., Stevenson v. Union Pacific R. Co.*, 354 F.3d 739, 748 (8th Cir. 2004) (court imposed adverse inference instruction when defendant failed to preserve voice tape of train crew at time of accident because defendant should have known that the tape would be relevant to litigation).

25 *Residential Funding Corp. v. DeGeorge Home Alliance, Inc.*, 306 F.3d 99, 113 (2d Cir. 2002). The negligence in this case consisted of plaintiff's failure to produce e-mails after the trial had begun, claiming that its vendor was unable to retrieve them from backup tapes, failure to mention to defendant that documents from critical time frames were not produced, and plaintiff's failure to meet a deadline to mail backup tapes to defendant's vendor, all of which hindered discovery. *See id.* at 110.

26 *Qualcomm Inc. v. Broadcom Corp.*, No. 05cv1958-B, 2008 U.S. Dist. LEXIS 911, at *4, *63 (S.D. Cal. Jan. 7, 2008) (the court noted that because the attorneys' fee sanction was so large, it did not find an additional sanction imposed upon Qualcomm itself necessary, and noted "[i]f the imposition of an $8.5 million dollar sanction does not change Qualcomm's conduct, the Court doubt an additional fine would do so.")

27 *Qualcomm Inc. v. Broadcom Corp.*, No. 05cv1958-B, 2010 U.S. Dist. LEXIS 33889, at *9 (S.D. Cal. Apr. 2, 2010). Although the Court ultimately lifted sanctions with regard to certain outside counsel, the Court nonetheless found that the discovery failures were due to "an incredible breakdown in communications" between the attorneys and client. *Id.* at *10. The *Qualcomm* case still serves as a reminder that discovery obligations are of significant interest to American courts.

28 *See Coleman Holdings, Inc.*, 2005 WL 67071, at *1.

8,000 pages of e-mail) were not released to plaintiff.[29] Additionally, once it discovered the additional tapes, Morgan Stanley was found to have continued to frustrate discovery by failing to produce the tapes in a timely manner. The court considered Morgan Stanley's failure to locate the back up tapes in a timely fashion, or in readily accessible form, to be gross negligence.[30] As a result, the court granted plaintiff's motion for an adverse inference instruction and ordered Morgan Stanley to continue to use its best efforts to produce additional tapes.[31]

6. Sedona Principles

The "Sedona Principles Addressing Electronic Document Protection" published by the "Sedona Conference"[32] provide some additional guidance for the handling of ESI in the context of an e-discovery exercise taking place in the U.S. These principles, which are not legally binding but nonetheless acknowledged in the U.S., describe the parties' obligations in the context of e-discovery. Nos. 1, 3, 5, 6, 8, 9 and 12 deal with the obligation to store data and state that parties to an e-discovery exercise should not request data which has already been deleted or which would need to be restored (No. 8).

II. The British Concept of E-Disclosure

1. U.S. v. UK Style Discovery

The terms "discovery" and "disclosure" are commonly used in both the UK and the U.S. to describe the process of pre-trial evidence collection and production. This terminology can be confusing. In both the rules governing civil litigation in England and Wales, the Civil Rules of Procedure (CPR) and in the Federal Rules of Civil Procedure (FRCP) as outlined above, the term "disclosure" refers to each party's duty to provide other parties with certain categories of information. In the U.S., however, documents subject to initial "disclosure" are fairly limited in scope and generally do not include documents that may be damaging to one's own case.

In England and Wales, each party must disclose documents on which it relies and which support or adversely affect either its case or another party's case. This therefore includes adverse and damaging documents. This is known as "standard disclosure" and replaces the former (and wider) definition of "relevance" as the basis of disclosure. In almost every case, each party must make this "standard disclosure" by way of a list which identifies documents which are in existence (or once existed in the past but which have since been lost or destroyed) and which fall within the definition of "standard disclosure". A party is required to disclose only those documents (i) on which it relies; (ii) which adversely affect its case; (iii) which adversely affect the other party's case; (iv) which support the other party's case; or (v) which are required to be disclosed in specific circumstances by particular court rules. The scope of this disclosure is narrower than under the previous rule and was thereby intended to reduce the costs associated with disclosure.

In assessing what is disclosable material, a party has a duty to make a "reasonable search", in proportion to the sums in issue and the costs of carrying out the search and to make a disclosure statement, verifying the extent of the searches that have been carried out. The legal representative has the duty to ensure that the person making the statement understands the duty of disclosure applicable to his client. If a party believes that another party has any specific documents which he has failed to disclose, he may make an application for "specific disclosure". In both "standard disclosure" and "specific disclosure", the duty of disclosure is limited to documents that are, or have been, in a party's control. Therefore, documents which have been lost or destroyed need to be considered as documents held by third parties in respect of whom there is a right to compel documents to be handed over.

As set out before, in the U.S., "disclosure" is followed by "discovery" (via, e.g., document requests pursuant to FRCP 34), whereby parties have an opportunity to seek additional information, from each other and other sources, through several avenues, including specific document requests, depositions, interrogatories, and on-site inspections. Where information is properly requested by one party during U.S. discovery, the responding party is generally under a duty to produce them, unless the producing party can raise convincing arguments to the contrary. Hence, the U.S. approach is less voluntary and puts more of a burden on a party to frame its discovery requests than the UK system does. Under the English system there is also a system of obtaining pre-action disclosure in certain limited cases. The main difference between the two, however, relates to the deposition process, which features prominently in the U.S. system and not at all in the English system where witness statements are used.

2. The Duty to Preserve in UK Law

In the UK, at minimum, the duty to preserve arises when litigation has commenced.[33] There has been some debate in the legal profession about whether it arises earlier. It was noted in the recent judgment of *Earles v. Barclays Bank* that "there might be cases where it was appropriate to draw adverse inferences from a party's conduct before the commencement of proceedings."[34] This is if there has been deliberate spoilation of evidence. The court noted that given the abundance of ESI potential litigants need to anticipate having to give disclosure of relevant electronic documentation and the means of doing so efficiently and effectively.

In practice, an organisation would do well to treat the obligation as arising as soon as it is reasonably believed that a dispute (and therefore litigation) might arise. A failure to preserve in these circumstances runs the risk of the future opponent arguing that the concept of adverse inference should apply. Equally, a party contemplating the bringing of a case should in practice write as early as possible to the opponent to put them on notice that relevant documents should be preserved in order to give rise to the possibility of arguing for an adverse inference if documents are not in fact properly preserved.

29 *See id.* at *3.
30 *See id.* at *5.
31 *See id.* at *7.
32 The Sedona Principles Addressing Electronic Document Protection is available for download at the Sedona Conference's website, *www.thesedonaconference.org*.
33 *Rockwell Machine v. Barrus* [1968] 1 W.L.R. 693.
34 [2009] EWHC 2500 (Mercantile).

3. Sanctions in the UK

UK lawyers must ensure that relevant electronic documents are adequately preserved in order to avoid the possibility of sanctions being issued for data spoliation. The principle has been upheld, or at least considered, in a handful of English and Irish cases, including more recent cases.The power to impose sanctions may include the striking out of claims, costs awards, the drawing of adverse inferences or a contempt of court. However, even where destruction has been deliberate, the UK Courts have emphasized that the purpose of these "sanctions" is not to punish, no matter how deplorable the conduct of the defaulting party may be. The ultimate test is whether a fair trial remains possible notwithstanding the default.[35] In *Douglas and Others v. Hello! Ltd and Others*[36], the court drew a distinction between documents which are destroyed or disposed of before proceedings have commenced and where they are destroyed afterwards. Regarding documents destroyed before proceedings have commenced, the court followed the test applied in *British American Tobacco Australian Services Ltd v. Cowell and McCabe*[37], namely, had the destruction or disposal amounted to an attempt to pervert the course of justice.

In the UK, the recent case of *Timothy Duncan Earles v. Barclays Bank*[38] indicates that the judiciary is becoming increasingly strict about the need to disclose ESI in litigation. In this case, the court was of the view that contemporaneous documents were critical. The events took place three years prior to the trial and it was not realistic to expect people to remember with reliability what was said. The bank did not put in place a litigation hold, in other words take steps to preserve records after litigation was anticipated. Telephone records and other documents recording instructions were not produced during pre-trial disclosure and this was described as a "gross omission". Because information was not deliberately withheld to obtain a tactical advantage, no adverse inferences were drawn against the bank. Nevertheless, the court was critical of the way in which the bank conducted its disclosure of documents saying that evidence should have been retained. A reduction of 50 % in the costs recoverable by the bank was a direct consequence of its failure to efficiently disclose electronic documents. The court felt that an organisation such as the bank had no excuse for not having the systems and procedures in place to retain information required in litigation.

4. UK Case Law

In addition to the cases noted before, there has been very little case law in the UK dealing with the application of disclosure rules in practice. The following cases illustrate the approach of the courts in recent cases.

In October 2008, three years after the 2005 amendments to the Civil Procedure Rules, a long-awaited decision was reported on the application of the rules, in the case of *Digicell (St Lucia) Ltd and Other Companies v. Cable and Wireless plc and Other Companies*[39]. The case deals with the scope of the reasonable search for electronic documents, key word searching, access to back up tapes, cost shifting and the importance of the parties' co-operation with each other. The case concerned disputed access to a series of back up tapes believed to contain e-mail accounts of former employees. Standard disclosure had already been given. The Court made it clear that what constitutes the reasonable search is ultimately a decision for the judge to make either before a search has been carried out or (as in the instant case) with the benefit of hindsight afterwards. Having regard to the factors specified in CPR 31.7 and paragraph 2A.4 of the Practice Direction, the Court decided that controlled access to the back up tapes was appropriate. The parties were directed to discuss with the help of technology consultants how this could best be achieved. This underscored the requirement in Paragraph 2A.2 of the Practice Direction that the parties should discuss electronic sources and should request assistance from the Judge, if difficulties arise, before the first Case Management Conference.

In *Abela v. Hammonds*[40], a solicitor's computer appeared to contain nothing and so the computer was destroyed. The court was suspicious as to the computer containing no documents at all. Hammonds may have been able to better justify its decision if an expert had signed off on the fact the computer did not contain any data before the hardware was destroyed. Alternatively, if they thought that there was some relevant data, a forensic investigator could have taken a forensic image of the hard disk and reported as to whether documents or data were recoverable.

Hedrich v. Standard Chartered Bank [2007] EWHC 1656 (QB) and on appeal *[2008] EWCA 905* is a good example of what can go wrong if the lawyers do not get an early grasp on electronically stored information in English litigation. The lawyers were forced to withdraw at trial when damaging material emerged far too late in the process. This case emphasises that the professional obligations of disclosure are owed to the court by the lawyers on the record just as much as by the parties to the lawsuit and cited *Myers v. Elman [1940] AC 282*, a case on disclosure which still stands as the leading authority on professional misconduct by solicitors. The *Earles* case is discussed above and along with the other cases referred to before indicates that the judiciary in the UK is becoming increasingly strict about the need to disclose ESI in litigation.

III. E-Discovery in Continental Europe, especially in Germany and France

1. Enforceability under the Hague Convention

It may be the case that a disclosure obligation originating from the U.S. or UK may also comprise documents in the possession and control of European companies, based on the understanding that they may have possibly received some relevant documents. It follows that also companies seated in Europe might be faced with e-discovery requests or regulatory orders to produce electronic documents. This is especially the case if such firms are e.g. subsidiaries of American corporate groups ("alter ego theory") or if they operate abroad

35 *Arrow Nominees Inc v. Backledge [2001] BCC 591.*
36 [2005] All ER (D) 280 (May), [2005] EWCA Civ 595.
37 [2002] VSCA 197.
38 [2009] EWHC 2500 (Mercantile).
39 *Digicell (St Lucia) Ltd and Other Companies v. Cable and Wireless plc and Other Companies* [2008] All ER (D) 226 (Oct).
40 *Abela and others v. Hammonds Suddards (a firm) and others* [2008] All ER (D) 22 (Dec).

(by "doing business" or establishing "minimum contacts" for example).

However, it is unlikely that formal e-disclosure production requests will be successful as they will be facing procedural obstacles such as the *Hague Convention on the Taking of Evidence Abroad*.[41] Among other states in the European Union[42], Germany has raised a reservation under Article 23 of the Hague Convention not to deal with requests for legal assistance to be given in the context of pre-trial discovery taking place in Common Law countries.[43] Therefore, requesting official assistance for the production of ESI on an European authority level are likely not to be successful. Hence, at least by virtue of the Hague Evidence Convention, litigants from the U.S. or UK could not impose any direct enforceable obligation of assistance on German companies.

American courts and U.S. attorneys, however, do not always seem to regard the stipulations contained in the Hague Convention or applicable privacy rules as imperative. As a recent example, in the breach of contract case *Accessdata Corp. v. Alste Techs. GmbH* the defendants objected to disclosure of ESI related to the case since disclosure would be blocked by German law and the Hague Convention rules. The basis of their objection was that it would be a "huge breach of fundamental privacy laws in Germany" and subject the defendants to "civil and criminal penalties for violating the German data protection law and the German Constitution."[44] The Court explicitly disagreed and ordered disclosure of ESI even assuming that the German privacy law prohibited disclosure of personal third-party information. It argued that the United States Supreme Court had addressed this issue in *Societe Nationale Industrielle Aerospatiale v. United States District Court* where the Supreme Court held that "it is well settled that such [blocking] statutes do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute."[45]

In another European case, this time relating to France, namely *Strauss v. Credit Lyonnais*[46], Magistrate Judge Kiyo Matsumoto upheld an previous order which mandated disclosure of documents from a French bank in relation to a terrorist attack in Israel. The defendant even sought a protective order using as justification a letter received from the French Ministry of Justice which stated that discovery not in compliance with the Hague Convention would result in a "violation of the sovereignty of the French State." Disregarding the defendant's additional contention that violation of the Hague Convention would even result in criminal sanctions, the court cited the Restatement (Third) of Foreign Relations Law of the United States, § 442, which sets forth five factors to consider regarding the disclosure of foreign documents that are relevant to U.S. disputes.[47] Based on these factors, the court finally denied the defendant's motion.

Accordingly, in spite of the German or other EU Member States' reservations made under the Hague Convention or other applicable rules, sometimes it is just being neglected that the Hague Evidence Convention is basically applicable for production requests and that European companies may face severe data protection sanctions when complying with such requests. Nevertheless, European companies sometimes adhere to such instructions due to a fear of facing sanctions, for commercial/financial reasons, or perhaps because they have an interest in the process of pre-trial-discovery taking place abroad, without even considering applicable data privacy rules.

2. Data Protection Issues

To avoid procedural sanctions and still to comply with applicable privacy regulations it has proven to be helpful to present to the court a comprehensive legal opinion elucidating the imperative rules of European privacy laws and showing that e-discovery requests can be in clear violation of mandatory law. In essence, at least where there is a true conflict between American law and that of a foreign jurisdiction, applicable conflict of law rules will require the court to conduct a comity analysis.[48]

a) Legal Regime in Germany

Under the compulsory requirements of German data protection laws, the disclosure and transfer of personal data is generally prohibited. This principle is based on the German Constitution *(Grundgesetz)*. Furthermore, the German Constitutional Court *(BVerfG)* holds that there exists a fundamental right of the individual to "informational self-determination". In addition, German privacy law is inspired by the principles of data prevention and data economy, i.e. as little personal data as possible should be collected, processed and used.[49] This gives the individual the right to control any third party access to its personal data and is recognized under German law as a high ranking, fundamental right and principle.[50]

These constitutional rights of the individual have been reflected and codified in the German Federal Data Protection Act (German DP Act) as recently amended with

41 Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, Mar. 18, 1970, 23 U.S.T. 2555, T.I.A.S. No. 7444, 847 U.N.T.S. 231 (1972).

42 *See* e.g. relating to France the "Délibération n° 2009-474 du 23 Juillet 2009 portant recommandation en matière de transfert de données à caractère personnel dans le cadre de procédures judiciaires américaines dite de "Discovery", published August 19, 2009, *http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020981625&categorieLien=id*.

43 It is not clearly established whether this reservation would also apply in the context of e-discovery, as "documents" and ESI are not treated as being equivalent under the FRCP. It is also important to note that e-discovery was not known in Germany at the time the *Hague Convention* became applicable and when the German reservation was made. Before Rule 34(a) of the FRCP came in force in December 2006, electronically generated data was not differentiated from any other type of data.

44 *Accessdata Corp. v. Alste Techs. GmbH*, 2010 U.S. Dist. LEXIS 4566 (D. Utah Jan. 21, 2010), MMR 2010, p. 275 et. seq.

45 *Id.* at 544 n. 29.

46 249 F.R.D. 429 (E.D.N.Y. 2008).

47 These factors which US courts consider in deciding whether to issue an order directing production of information located outside the US are: (1) The importance to the investigation or litigation of the documents or other information requested; (2) the degree of specificity of the request; (3) whether the information originated in the US; (4) the availability of alternative means of securing the information; and (5) the extent to which non-compliance with the request would undermine important interests of the US, or compliance with the request would undermine important interests of the state where the information is located.

48 Pursuant to Rst. § 442, the court should also weigh the extent to which ... compliance with the [discover] request would undermine the important interests of the state where the information is located, *Maxwell*, 93 F3d at 1050; *Hilton v. Guvot*, 159 U.S. 113, 143, 16 S.Ct 139, 40.

49 See Section 3 lit. a) German DP Act.

50 *See Gola/Schomerus*, BDSG, Kommentar, 9th edition 2007, § 1 no. 3.

effect of September 1, 2009 (NB: new legislation is likely to come into force not later than the end of 2010).[51] This legislation specifically applies to electronically stored information (ESI) containing personal data which has or will be collected on the German territory. It follows that the collection, processing and disclosure of private data collected on the territory of Germany – also in the context of an e-discovery – underlies the restrictions of the German DP Act.[52] In contrast to some privacy laws overseas[53], the German data protection law (which is derived from the European Data Protection Directive 95/46/EC) protects the individual against his rights to privacy being impaired through the handling of his personal data. Therefore, a data controller (in most cases the employer) is under full responsibility to collect, process and use (which includes the transfer) personal data contained in electronic files. Violations of the German DP Act may be prosecuted as administrative or criminal offence (according to Section 43 German DP Act the former are punishable by fines and the latter, according to Section 44 para 1 German DP Act, even by imprisonment for up to two years).[54] Besides, the protected provisions of the German DP Act may also be enforced by the individual data subjects (Section 34 German DP Act) as well as the competent data protection authorities (Section 38 German DP Act).

b) Balancing the Interests

In essence, this means that the collection, production and transfer of personal data can only be carried out if permitted by the German DP Act or any other German legal provision or in case the data subject has explicitly consented.[55] Furthermore, as regards the discovery of personal data from employees, this is only possible under the strict regulations of Sections 28 and 32 German DP Act. Under the recently amended Section 32 German DP Act, the processing of personal data of current employees and also former staff is only permitted under certain, very limited circumstances.[56] This means that the respective data controller must balance the protection of the employees' rights with the purpose for which such processing is being required and determine whether it is used for the purpose of the employment relationship. It follows that Section 32 German DP Act itself does not allow the production and transfer of private data for an e-discovery process. However, section 28 para 1 No. 2 German DP Act, if and as far as it is applicable besides the *lex specialis* Section 32 German DP Act, i.a. states that the collection and storage of data may be permissible if required for the safeguarding of legitimate interests (e.g. in the context of legal proceedings) and if it is balanced with the rights of the data subjects.[57] Therefore, before searching for and producing e-mails that may contain personal data the German company must also balance the protection of the employees' rights (considered as data subjects) with the purpose for which such processing is being required. This exercise has to be carried out on a case by case basis.

c) Actual Transfer of Data

Even if the collection of electronic data has taken place, the following transfer of the relevant ESI to the U.S. may also be problematic.[58] Under Section 4 b para 2 of the German DP Act, a cross border transfer of data from Germany to a foreign country may only be carried out if an adequate level of data protection is guaranteed in the country in which the data is to be transferred. It is important to note that at least under German law the level of data protection existing in Germany is not considered to be the same as in the U.S. Furthermore, such transferred data could only be used in the context of legal proceedings. However, there is a principle in the U.S. that data exhibited as part of legal proceedings has to be made available to the members of the public upon request. This principle would also conflict with the requirements of Sections 4 b and 4 c of the German DP Act.

d) Secrecy of Telecommunication and Co-Determination of Works Councils

It follows that at least unlimited e-discovery request will not be fully compatible with European, especially German privacy law. The fact that many employees at companies are permitted to use e-mail and internet for their own personal use even render the situation more complicated as in such situations, the employer is treated as a provider of telecommunication services under the German Telecommunications Act and is therefore obliged to protect the secrecy of telecommunications. It is important not to forget that also a works council (if any should exist within the company) has certain rights of determination in connection with the use of e-mails and internet access of the employees under the German Works Constitution Act. In most cases, the collection and transfer of any such personal data will have to be first discussed with the relevant works council and the data protection officer at an early stage of the e-discovery exercise.

IV. An Irreconcilable Difference in Law?

For all the reasons discussed above, EU/German privacy law and U.S./UK law on e-discovery seem to be incompatible. However, instead of completely refusing to satisfy a disclosure request on the ground of the existence of

51 BGBl. I, p. 66, as amended by BGBl. I, p. 160 (BT-Drucks. 16/12011; BT-Drucks. 16/13657).

52 *See Rath/Klug*, E-Discovery in Germany, K&R 2008, 596 (598).

53 *See* Sedona Conference Framework for Analysis of Cross Border Discovery Conflicts – A practical guide to navigating the competing currents of international data privacy and discovery – April 23, 2008 (Public Comment Version), A Project of the Sedona Conference Working Group 6 on International Electronic Information Management, Discovery and Disclosure, *www.thesedonaconference.org/dltForm?did=WG6_Cross_Border.*

54 *See Gola/Schomerus*, BDSG, § 43 no. 16.

55 Only exceptionally, it might be permitted under German law to collect, produce or use personal data without fulfilling these categories. However, these exemptions may only be used very restrictive in order to comply with the principle that under German data protection law any collection, process or use of personal data is basically prohibited unless explicitly allowed, s*ee Simitis*, BDSG, § 28 no. 133.

56 Section 32 para 1 sentence 1 German DP Act reads as follows: "Personal data of an employee may only be collected, processed or used for the purposes of the employment relationship if this is necessary for the decision of the establishment of an employment relationship or, after establishment of an employment relationship, if this is necessary for its performance or termination."

57 Section 28 para 1 No. 2 German DP Act reads – in its relevant parts – as follows: "The collection, storage, modification or transfer of personal data or their use as a means of fulfilling one's own business purposes shall be admissible 1. [...], 2. in so far as this is necessary to safeguard justified interests of the data controller and there is no reason to assume that the data subject has an overriding legitimate interest in his data being excluded from processing or use, [...].

58 *See Rath/Klug*, E-Discovery in Germany, K&R 2008, 596 (598).

a conflicting national data protection legislation, it should be considered to find a privacy compliant approach. One approach could be Rule 26(c) of the FRCP. Under this Rule, the court can set aside or limit a disclosure obligation in an effort to protect a party from undue burden, annoyance, embarrassment, or expense.[59] This could be affected by an order prohibiting the disclosure of such data or specifying that the documents to be disclosed should be handed over to the court under seal.

1. Guiding Principles

It is also helpful to know that the "Article 29 Data Protection Working Party" of the European Union as well as the German equivalent, the so-called "*Düsseldorfer Kreis*", have in the meantime issued some additional guidance in how to proceed in cross border e-discovery cases.[60] The EU Working Party has recently adopted the "Working Document 1/2009 on pre-trial discovery for cross border civil litigation (WP 158)"[61] providing guidance to data controllers subject to EU law in dealing with requests to transfer personal data to another jurisdiction for use in civil litigation. In this document, the Working Party recognizes that the parties involved in litigation may have a legitimate interest in accessing information that is necessary to make or defend a claim, but also constitutes that this must be well balanced with the rights of the individual whose personal data is being sought.[62] The Working Party furthermore sees the need for reconciling the requirements of the U.S .litigation rules and the EU data protection provisions, but also confirms that where data controllers seek to transfer personal data for litigation purposes, there must be compliance with applicable data protection requirements (for Germany this means the observance of the German DP Act as set out before). Therefore, also in the opinion of the EU Working Party, in order for the pre-trial discovery procedure to take place lawfully, the processing of personal data needs to be legitimate and to satisfy the grounds set out in Articles 7 and 26 of the Data Protection Directive which have been duly implemented into German data protection law as set out above.

In essence, the Working Party as well as the Düsseldorfer Kreis hold that an obligation imposed by a foreign legal statute or regulation (such as Art. 26 FRCP) would not qualify as a legal obligation by virtue of which data processing relating to e-discovery requests could be made legitimate. The Working Party also confirms from an EU perspective that there is a unalienable duty upon the data controller (the company) involved in litigation to take such steps as are appropriate (in view of the sensitivity of the data in question and of alternative sources of the information) to limit the discovery of personal data as much as possible and to that extent which is objectively relevant to the issues being litigated. Also, where it is adequate for the Hague Convention to be followed, the Working Party urges that this approach should be considered as a method of providing for the transfer of information for litigation purposes.

2. Document Retention Policy

Until the conflicting situation is clarified on a legal and cross border level, companies located in Europe that could be involved in the production of ESI have no choice but to implement their own internal document retention procedures to secure all relevant evidence. The deletion of electronic data should also be controlled across any group of companies, in compliance with the applicable data protection law and should be suspended as soon as a legal dispute becomes foreseeable or if such data is otherwise required for any other purpose.

A "DRP" (as already shown in part 1 of this article) can be a suitable tool to implement a standardised procedure for the handling, archiving and deletion of electronic data within a company. Such policy can remedy the problem of securing storage and mediate the risk of early deletion. In case of German companies doing business abroad, such policy could also be drafted in accordance with the spirit of the FRCP. For instance, Rule 37(f) of the FRCP, the Safe Harbor Rule, protects a party from potential sanctions if such party is not able to disclose certain ESI due to the fact that the ESI was lost as a result of a routine operation performed in good faith within an electronic information system.[63]

The rationale behind the Safe Harbor rule is that companies in some instances must delete some ESI because permanent storage of ESI could overwhelm a company in size and cost. For example, in *Zubulake IV*, plaintiff moved for sanctions in part due to defendant's failure to preserve all relevant back up tapes.[64] The court stated that a litigation hold "does not [generally] apply to inaccessible back up tapes... which may continue to be recycled on the schedule set forth in the company's policy" but if tapes are accessible, then such tapes are subject to the litigation hold.[65]

The Safe Harbor exemption applies to policies involving automatic removal processes as well as manual processes. Additionally, the rule is only applicable if the company's guidelines are comprehensible and the dele-

59 *See* Fed. R. Civ. P. 26(c), *Duty to Disclose*; *General Provisions Governing Discovery.*

60 The Article 29 Data Protection Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. Further information can be found at *http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm*. The "Düsseldorfer Kreis" can be regarded as the German equivalent to such EU Working Party, being a convention of representatives of the German data protection authorities. The Düsseldorfer Kreis has i.a. recently assessed that Section 4 c Abs. 1 Sentence 1 No. 4 BDSG does not provide legal grounds to support a data transfer related to e-discovery requests. Further information can be found at *www.datenschutz-berlin.de/content/themen-a-z/internationaler-datenverkehr/datenuebermittlungen-an-us-behoerden-sowie-us-unternehmen*.

61 *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp158_en.pdf*.

62 The Working Party already considered the effects of the Restatement (Third) of Foreign Law of the United States no. 442 and the various decision of U.S. courts acknowledging that a balancing exercise should be carried out with the aim that the trial court should rule on a party's request for production of information located abroad only after balancing: (1) the importance to the litigation of the information requested; (2) the degree of specificity of request; (3) whether the information originated in the U.S.; (4) the availability of alternative means of securing the information; (5) the extent to which non-compliance would undermine the interests of the U.S. or compliance with the request would undermine the interests of a foreign sovereign nation; see id, p. 5 et seq.

63 *See*, e.g., *Morris v. Union Pacific R.R.*, 373 F.3d 896, 901 (8th Cir. 2004) (court held that because there was no showing that the destruction of evidence was done with intent to suppress the truth, the sanction of an adverse inference is not proper).

64 *See Zubulake IV*, 220 F.R.D. 212 at 216.

65 *Id.* at 218. *Coleman Holdings, Inc.*, 2005 WL 67071, at *5. (held that defendant acted grossly negligent by failing to locate certain back up tapes in a timely matter).

tion of data does not aim to serve the purpose of withholding data from a possible future legal opponent. This basically means that potential targets of e-discovery requests are well advised to implement up-to-date DRP as these policies would show that they have considered applicable data protection law, but would also allow them to draft their policies on the basis of the requirements of Rule 37(f) of the FRCP. It follows that implementing a DRP may be one strategic instrument to remedy this general conflicting issue.

V. Technologies and Technical Expertise to Support E-Discovery

1. Achieving Proportionality in E-Disclosure

It is equally important not to neglect the technology aspects of e-discovery as there is a real risk of legal costs spiralling out of control as parties go through the process of locating and disclosing electronic documents. An uneasy tension arises between the need to minimise legal cost and the need to satisfy judges or regulators expectations about the quality of the disclosure made. There is clearly a need to follow an efficient process to minimise cost and justify efforts. This is where technology comes into the equation, helping locate, reduce and review relevant evidence efficiently.

Ensuring that the scope of the search is proportionate to the case at hand requires lawyers not only to comply with data protection issues, but to weigh up the value or significance of the case against the significance of the evidence that might be found and the cost of retrieving it. Parties are discussing this with the other side and are using early case assessment tools and data culling technologies to help reduce the volume of potentially relevant documents and identify those that are relevant. They are also calling for cost estimates from technology providers to support their arguments. It is also important for each party to ensure that its document review is well structured so that the right sort of documents are reviewed by appropriate members of the legal team and time is not wasted by senior lawyers at high charge out rates reviewing large volumes of irrelevant documents which can be handled by paralegal staff. Parties therefore often adopt a staged approach to the review of electronic documents which is always a good move from a data protection perspective.

2. How to Locate and Preserve Data

Given the large universe of potentially relevant electronic evidence, the challenge in evidence management is to target the key documents. Technology offers efficient solutions to help control the volumes and increase speed, accuracy and efficiency that comes from working electronically. Collecting electronic data in a discovery exercise can still be a daunting task due to the wide variety of electronic storage locations, the vast amount of data available and the ever-increasing file types used in business. Identifying the most relevant electronic evidence can be a complex process. Technology experts under guidance from legal teams are able to help navigate the corporate IT systems and extract the required information in a systematic way. Once litigation is anticipated, steps should be taken to safeguard evidence (litigation hold) and avoid loss of data. This may involve imaging laptops of key individuals or removing restrictions on the size of mailboxes for key individuals to avoid the risk of data being routinely deleted when the limits are reached. Once these immediate preservation steps have been taken the legal team can then identify and collect those sources of data that are potentially relevant to the proceedings and that needed to be reviewed.

3. Identifying the Key Evidence

The careful selection of data locations to be searched across lays the foundation for proportionality and data protection in an e-discovery exercise. Taking data protection seriously means restricting the places and sources that need to be searched by selecting relevant locations, departments and individuals and then, looking for the storage devices, electronic folders and files likely to contain relevant information. Lawyers will set about the task of working out who the key individuals are, what types of documents are likely to be relevant and which time periods are material. In order to make decisions about the collection of data it helps to map out the company's IT infrastructure (the operating systems in use, the hardware, software and storage areas) and the flow of information into and out of the company. Also important is information about the company's backup protocols and procedures followed to retain or destroy data when individuals leave the company. The aim is to establish where and how information is created, stored, backed up and purged. Forensic experts are able to help lawyers obtain the information they need so that they can work out with a greater degree of precision how best to preserve and collect documents.

4. Collection Options

Several data collection options are available, and the best method will vary depending on the specifics of the situation. Options include having an expert perform an onsite data collection or using "do-it-yourself" data collection software to collect the data. In smaller cases, where the veracity of the electronic evidence is unlikely to be challenged, it is not uncommon for companies to collect their own data and then hand it to an external service provider for data processing and delivery into a database for review by the legal team. In other cases external forensic experts are relied upon to collect data, particularly when neutrality and strict forensic procedures or investigation is required (for example, in dealings with regulators or when misconduct is suspected). In such cases it is essential to show that evidence has been properly preserved and captured and not contaminated in any way. Forensic experts are also typically used when it is necessary to go onsite simultaneously in multiple jurisdictions to quickly and efficiently capture crucial evidence from a wide variety of systems and media with minimal business disruption. Whichever method is chosen, the initial data collection steps can be the most critical part of an investigation and impact on the subsequent analysis of evidence. Missteps can be costly for a case or investigation because of loss of evidence or risk of sanctions for not collecting the evidence in the most appropriate way suitable to the needs of the case. Significant planning, the right equipment and procedures and training are essential to ensure that data collection is carried out properly and the risk of damaging, deleting or missing data avoided.

5. Social Networking and Cloud Computing

The collection of data will become more complicated as data no longer resides on servers under a company's direct control but has disappeared into a web-based cloud as data management is outsourced. "Where is it" has become the key question and is it possible to access key information if it is needed in a dispute. It is also now necessary to think about whether key data is going to be found in less formal communication channels like MSN Messenger or office communication tools like it allowing impromptu and spontaneous remarks. The question is whether material evidence can also be found on social networking sites like Twitter, Facebook and Myspace. These new sources of evidence pose interesting legal and technical questions as to whether this is disclosable data and how to deal with privacy rights and admissibility. In recent cases in the U.S. and Canada, even social networking information has been used in litigation.[66]

6. Filtering and Searching Technologies

Not every electronic document found on a custodian's computer or on backup tapes is relevant to a disclosure production and admissable from a data protection perspective. Data filtering technologies help reduce the potentially enormous universe of data to a manageable and relevant sub-set for review and production. The time spent by lawyers reviewing documents can be significantly reduced by relying on the following filtering processes: Custodian selection, date filtering, keyword searching, de-duplication and removal of system and program files, large files and blank pages. The search engines underpinning data filtering engines are many and varied and include "and" and "or" Boolean searching as well as cutting-edge concept searching engines. During this stage of the e-discovery process the legal team produces a list of keywords which is used to filter the data and identify potentially relevant documents.

Once the data has been filtered relevant documents are loaded into a database for review. Documents can be made available in their native format – in other words in the original format in which they were created. It is also possible to convert the filtered set of documents to be reviewed into image format such as TIFF images (Tagged Image File Format) or PDF (Portable Document Format). The technologies used by external providers of electronic disclosure services are sophisticated and in some cases are supported by a complex hardware infrastructure allowing them to process millions of pages a day.

7. Early Case Assessment Tools

Early case assessment tools are available and provide early visibility of the data that might be relevant to a case before actually reviewing such documents. So before full data filtering or document review takes place data can be loaded into a first-pass review tool and selections can be made about which data sources to focus on. This process significantly reduces the size of document collections and the related costs of e-discovery. Reducing the data in an intelligent and potentially privacy compliant way before more expensive processing costs are incurred is an effective means of controlling costs and complying with data privacy laws. Advanced e-mail analysis features are available in some of these early case assessment tools and provide graphs which show the volume and frequency of e-mail traffic. This makes it possible to see quickly who has been communicating a lot with whom, when and about what. This may, however, give rise to additional data protection issues.

It is also possible to see the results of keyword searches that have been run against various e-mail boxes. For every word run you can see which individuals' e-mails contained the word or phrase searched for and how many documents contained these "hits". This sort of statistical analysis helps lawyers adopt a more scientific approach to keyword searching and provides evidence for sensible discussions with the other side about the keywords that should be run against the data to select documents for discovery. After the early case assessment stage, machine filtering of the documents can be done to reduce volume with more reliability. The combination of human selection and machine filtering can reduce the volume of documents that need to be reviewed by lawyers significantly. Of course, early case assessment also supports the assessment of the merits of a case early on in proceedings allowing lawyers to decide early on in a case whether or not to pursue an action or settle, based on the available evidence.

8. Using Technology to Reduce the Risk of Contravening Data Protection Laws

Where data collected in Europe needs to be transferred outside the EU, companies can rely on computer forensic experts to harvest data onsite in a targeted way using onsite searching tools. They can also rely on sophisticated filtering technology to search across potentially relevant data to identify key data. This reduces the risk of sending personal data out of Europe and ensures that only that which is necessary for the legal proceedings is transferred in accordance with applicable data protection laws. To further reduce the risk, the reduced data set can be reviewed for compliance with privacy in Europe and sensitive files removed. Finally, references to individuals can be redacted out before the data is accessed by means of pseudonymization or anonymization.

66 In *People v. Liceaga*, 2009 WL 186229 (Mich. Ct. App. Jan. 27, 2009), the prosecution sought to admit photographs discovered on the defendant's MySpace profile of himself displaying a gang sign and the gun allegedly used to shoot the victim as evidence of intent. In *United States v. Villanueva*, 2009 WL 455127 11th Cir. Feb. 25, 2009), the Court found that post-conviction photos discovered on the defendant's MySpace page of the defending holding a semi-automatic gun with a loaded clip after the defendant had been convicted of a violent felony could be used as evidence to enhance sentencing. In *Bishop v. Minichiello*, B.C.J. No. 692 (S.C.J.) 2009), the Court in British Columbia found a plaintiff's late-night computer usage on Facebook (as recorded in the log-in/log-out records on his hard drive) was relevant evidence regarding his personal injury claim.