COMPUTER LAW REVIEW
International

CRi

Offprint

A Journal
of Information Law
and Technology

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

Irreconcilable Differences? Navigating Cross-Border E-Discovery

How best to understand and deal with the conflict between e-discovery and data protection principles

Verlag
Dr. Otto Schmidt
Köln

www.cr-international.com

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

Irreconcilable Differences? Navigating Cross-Border E-Discovery

How best to understand and deal with the conflict between e-discovery and data protection principles

Electronically stored information ('ESI') such as emails have become the corporate memory and central to fact-finding in lawsuits and investigations, providing an accurate and detailed record of what happened or what was said at any point in time. This also means that companies involved in litigation now have to disclose and produce these electronic communications and documents on short notice to comply with the rules of court governing pre-trial discovery. At the same time, the information stored in mailboxes or on company or even privately owned devices may well contain or be co-mingled with the personal and private data of company employees or other third parties. Europe has a long history of preserving the individual's right to privacy and has a complex network of legal rules designed to protect it including the restriction against transferring personal data across borders unless special conditions are met. This immediately causes difficulties in international litigation which relies on evidence scattered across jurisdictions. A conflict inevitably arises between the discovery laws of one country and the data protection laws of another. This article examines the challenges that arise when the discovery laws of another country clash with the data protection laws of another and how companies are addressing these challenges by relying on legal mechanisms and technology solutions.

In section I. the article provides an overview of the data protection framework in Europe and the discovery rules in the U.K. and U.S. and sets out the legal conflict which arises due to conflicting rights and obligations in these two legal regimes. The article examines in particular the impact of the U.K. Data Protection Act on disclosure rules in civil litigation conducted under the rules of court in England. In Section II., the article discusses the German data protection regime as a prominent example of civil law jurisdictions in the European Union and how it impacts on requests for e-discovery. The article highlights some of the data protection issues that arise and explores the enforceability of e-discovery requests in Europe. Finally, in Section III., the article explores how the conflict between e-discovery and data protection principles can be addressed in practice, especially when it comes to overcoming the prohibition or restrictions on cross-border data transfers. In doing so, the article looks at official guidance from data protection authorities and The Sedona Conference and at legal mechanisms such as obtaining the consent of individuals concerned, reliance on legal exemptions, binding corporate rules and data transfer agreements. The article also considers how technology can be used to facilitate international discovery and reduce the risk of contravening data protection laws.

▷ Karl Geercken and Kelly Holden are U.S. attorneys at Alston & Bird LLP, New York; Dr. Michael Rath is a German attorney, certified expert lawyer on information technology and partner at Luther, Cologne, Germany; Mark Surguy is a solicitor and partner at Eversheds, London, U.K.; and Tracey Stretton is a legal consultant at Kroll Ontrack, London, U.K. Further information abaout the authors at p. 63.

I. The Conflict Between Discovery and Data Protection Laws

Because discovery obligations cross territorial boundaries, a company in the U.S. engaged in litigation that needs to comply with the U.S. rules of court must disclose documents stored at its facilities or subsidiaries in other locations around the world. Similarly, a company in the U.K. involved in litigation must disclose documents stored on foreign countries. The European Data Protection Directive (95/46/EC) on the protection of individuals in relation to the automatic processing and free movement of personal data (the 'European Data Protection Directive') has been adopted into local law in the member states of the EU and sets out eight basic data protection principles which strictly control how 'personal data' is obtained, kept, processed and data transfers. Despite these laws many courts, especially those in the U.S. will still expect global discovery from parties to U.S. litigation that have international operations. Lawyers face the often difficult task of ensuring that discovery obligations are met while at the same time not violating the local laws of the place in which discovery is sought.

1. The European Data Protection Framework

The purpose of the European Data Protection Directive – until replaced by the European Data Protection Regulation a draft of which is currently being discussed[1] – is to harmonise the regulation of personal data in the European Union. The Directive essentially regulates the way organisations collect and use information about individuals and seeks to harmonise the position in Europe by directing how Member States should introduce national data protection legislation. The key premise is that the European Data Protection Directive regulates 'personal data' which is defined as 'any information relating to an identified or identifiable natural person' ('data subject'). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.'[2] This broad definition means that even names, birthdays, addresses, telephone numbers, fax numbers and email addresses are considered to be personal data. In the context of litigation, therefore, personal data is likely to be contained in any email or other document that is disclosed in the process of pre trial discovery. The Data Protection Directive also regulates 'processing'[3], which is essentially any type of activ-

1 The draft of the General Data Protection Regulation can be found at *http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf*.

2 Directive (95/46/EC), Art 2(a).

3 Directive (95/46/EC), Art 2(b): '... processing of personal data ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration,

ity one can contemplate with personal data. This means certain rules must be observed in all cases when data is collected from EU member states and then processed and reviewed for production in U.S. legal proceedings for discovery purposes.

The key provisions of the Data Protection Directive include:

- *Lawfulness and Fairness:* This requires that certain conditions must be satisfied in order to lawfully process personal data, with special controls in relation to 'sensitive' personal data;
- *Purpose Limitation:* This requires, for example, that data subjects are provided with a 'fair processing notice' and then the personal data is only processed as described in the notice;
- *Proportionality:* There must be limits to the processing of personal data that is undertaken, and this provision requires that user data is only processed if and to the extent that such processing is proportional in relation to the applicable circumstances;
- *Data Accuracy:* There is an obligation on those companies that are responsible for the personal data to ensure the accuracy of the personal data;
- *Data Retention:* Personal data, once collected, may only be retained in identifiable form for so long as is necessary in the circumstances;
- *Data Security:* All companies that handle personal data must implement appropriate technical and organizational measures to guard against unauthorized or unlawful processing of personal data and/or against loss or destruction of, or damage to, personal data;
- *Data Subject Rights:* This requires that data controllers respond to 'subject access requests' from data subjects, to provide information about the nature and scope of processing undertaken or to stop processing data in a way they can object to;
- *Data Transfers:* This requires, in summary, that the company may not transfer data outside the European Economic Area[4] ('EEA') to jurisdictions which do not ensure an adequate level of protection of personal data, without taking certain steps (e.g., implementation of model contractual clauses, obtaining data subject consent, obtaining the U.S. Department of Commerce Safe Habor certification or obtaining Binding Corporate Rules accreditation); and
- *Notification:* Most companies in Europe are required to register/notify as a 'data controller', if processing personal data in the context of an establishment in a member state. They may also need to notify if they seek to transfer personal data abroad.

Despite attempts to harmonise how personal data is regulated in the EU there are still a number of important local variances. These arise because of more stringent national data protection legislation in some countries, differing enforcement powers granted to national data protection authorities, variations in the way in which national courts approach data protection issues and finally by considerable differences in the way that data protection authorities approach infringement.

2. The Disclosure/Discovery Framework in Civil Litigation in Common Law Jurisdictions

The terms 'discovery' and 'disclosure' are commonly used in both England and the U.S. to describe the process of pre-trial evidence collection and production. 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'), the term 'disclosure' refers to each party's duty to provide other parties with certain categories of information. In the U.S., 'disclosure' is followed by 'discovery' (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.

3. E-Discovery in the U.S.

E-discovery occurs in the context of American 'pre-trial-discovery' or comparable procedures initiated in common law jurisdictions. 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' comprehensive information concerning all facts and evidence which could be 'relevant' to the alleged claim or defence (FRCP 26).[5] The definition of 'relevant' is broad; evidence may be relevant, for example, if it can *lead* to the discovery of useful evidence.[6] 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, which 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 (i.e. a request brought to a litigant by another party's lawyer to prepare and present relevant documents). Significantly, according to Rule 34 of the FRCP, ESI is governed by pre-trial-discovery regulations in the same manner as documentary evidence.[7] This means that a company's electronic information system (its servers, hard drives, backup systems, software document management systems and third party document

retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.'

4 The EEA includes all countries in the European Union, together with Iceland, Liechtenstein and Norway.

5 *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.').

6 *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.').

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

retention systems) is subject to discovery.[8] However, the FRCP offers little flexibility to limit the inclusion of such personal information.[9] FRCP Rule 5.2, for example, permits a party to redact[10] only the following: an individual's social-security number, taxpayer-identification number, or birth date, the name of an individual known to be a minor, or a financial-account number.

4. Sanctions in U.S. Courts for Infringement of the Discovery Obligation

A foreign company's failure to comply with U.S. discovery obligations due to data protection concerns could lead to considerable sanctions. U.S. courts are not unfamiliar with the differing data protection laws of many European countries and, as discussed in Section 4.1 below, U.S. courts employ a balancing test to determine whether a foreign entity must produce documents in a U.S. litigation case. Failure to comply with the court's decision could lead to sanctions such as 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), entering a judgment against the party in breach, permitting use of an adverse inference instruction to the jury, or ultimately dismissal.[11] Additionally, the party in breach may be ordered to pay considerable fines.

5. Disclosure in England

In England, each party must disclose documents on which it relies and which support or adversely affect either its case or another party's case.[12] 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[13] 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. 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 do documents held by third parties in respect of whom there is a right to compel documents to be handed over. It is permissible, subject to the discretion of the court on challenge by an opponent to redact parts of a disclosable document which are irrelevant or confidential. Strictly speaking if the document as a whole is within the scope of the disclosure obligation, confidentiality and irrelevance (unlike legal professional privilege) are not absolute objections to the obligation to disclose. Whilst it is not unheard of for personal information or sensitive information to be redacted in the context of litigation, it is an expensive process and would only be carried out for very good reason. The disclosing party would in most cases be entitled to rely on the protection of the court's order obliging disclosure to be given. It is worth noting that under the former system of civil litigation the rules obliged the parties to give automatic disclosure at a certain state of the proceedings whereas under the new regime the obligation only arises when the court makes an order. This enables the court to more strictly control the process.

A natural consequence of the existing approach to standard disclosure has been that a lawyer is required to review all documents gathered in the reasonable search before handing them over, a process which is costly given the large volume of documents now available and often disproportionate to the value of the case. A new Civil Procedure Rule CPR 31.5, introduced on 1 April 2013 makes provision for a menu of disclosure orders and disclosure directions, to allow for a more tailored approach in substantial cases. There will no longer be a presumption in favour of standard disclosure. Instead, the court must decide which of a range of orders to make ranging from dispensing with disclosure, to issue-based to disclosure and also full-blown "train of enquiry based" disclosure in appropriate cases. In selecting an appropriate order the court will take into account the overriding objective of the rules and the need to limit disclosure to that which is necessary to deal with the case justly. In the amendments to the CPR implemented on 1 April 2013, the overriding objective has been amended to include a reference to the need to deal with cases at a proportionate cost.

These amendments are being introduced in conjunction with a package of amendments including new cost man-

8 For example, a party to a lawsuit may rightfully request access to an opponent's emails relating to a certain time period or for documents containing certain key words. *See Coleman Holdings, Inc. v. Morgan Stanley*, No. 502003CA005045XXOCAI, 2005 WL 679071, at *1 (Fla. Cir. Ct. Mar. 1, 2005).

9 The FRCP does not directly address redactions in the context of document discovery. It does, however, offers guidelines regarding the redaction of certain personal information from documents filed with court, and law firms often mirror these guidelines in making decision to redact information from documents produced to opposing counsel.

10 To 'redact' a document means to remove part of the text of a document, typically by blacking it out and inserting the word 'Redacted'. Parties, for example, may redact certain words, numbers or sentences of a document. Redactions are most often done to prevent privileged material from being produced to an adversary.

11 Fed. R. Civ. P. 37, Failure to make Disclosures or to Co-operate in Discovery Sanctions. *See also Zubulake* Revisited, 2010 U.S. Dist. LEXIS 1839, at *24 (S.D.N.Y. Jan. 11, 2010) (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).

12 Civil Procedure Rule 31.6.

13 Civil Procedure Rule 31.7. Practice Direction 31 and Revised Practice Direction 31B set out various factors to be taken into account when assessing 'reasonableness'.

agement rules and together they are designed to keep the costs of litigation under control in line with the reforms suggested by Lord Justice Jackson following his review of the costs of civil litigation in the UK. The new cost management rules set out in proposed new rules CPR rules 3.12 to 3.18 and Practice Direction 3E will require parties to file and exchange budgets before the first case management conference for approval by the court. Costs will thereafter be actively managed by the court within the boundaries of those approved budget. At the end of a case the successful party will be able to recover the reasonable costs of the case and when these are assessed the court will take into account the approved budget.

6. How the U.K. Data Protection Act Impacts on Disclosure Obligations

The Data Protection Act 1998 in the U.K. implements the European Data Protection Directive. The Information Commissioner is the supervisory authority for the purposes of the Directive and Act. His duty is to promote best practice and the observance of the Act. This includes the production of codes of practice. The Act's 'protection' enables citizens to rely on the civil and political rights contained in the European Convention on Human Rights. The privacy of individuals with respect to the processing of relevant data is protected and the free flow of personal data in the interests of promoting trade is permitted. A balance therefore is required between these competing interests. The nature of the regulation was intended to be proportionate and not a box-ticking procedure.

When it comes to understanding the meaning of the Act it has to be interpreted in line with the policy of the Directive.

a) Compliance Duty on Data Protection Principles

The scheme of the legislation is that the 'Data Controller' is under a duty to comply with the 'Data Protection Principles'. The Data Controller is the person who decides how 'personal data' (i.e. data which relates to a living individual who can be identified) are to be 'processed'. Processing is a very wide term and effectively covers any activity to which the data might be subject (for example obtaining, recording, holding, retrieving data, as well as the use, adaptation, alteration, organization, disclosure, dissemination of data and making it available, consulting it erasing and destroying it). Any form of pre-trial disclosure to a party in litigation and even the collection and review work required in preparing to make disclosure constitute 'processing'. Importantly, the Act applies to any Data Controller who is established in the U.K. (ordinarily resident in or incorporated in any part of the U.K.). It also applies to a Data Controller that is established neither in the U.K. nor other EEA state, where equipment which is in the U.K. is used to process the data otherwise than for transition through the U.K.

b) Exceptions to Compliance Duty

Collecting and reviewing data in the U.K. for pre-action disclosure can generally be carried out within the confines of these exceptions without too much difficulty. The correct approach is therefore first to ask whether the processing in question is exempt from the duty to comply with the eight Principles. In order to understand the exceptions it is important to understand the distinction between the so called 'non-disclosure' provisions of the Act (broadly those of the eight Principles which restrict lawful data processing and which if not complied with may make the processing unlawful) and the 'subject information' provisions (those which confer the right on the data subject to ask for or to be notified about why his personal data is being processed). The way the exceptions apply depends on which of these two sets of provisions apply. Both sets of provisions would generally apply to disclosure in the context of litigation. Examples of the non-disclosure provisions are the requirements for the data processing to be proportionate and for the data processing to be for a specified purpose which is a lawful purpose. An example of the subject information provisions is the right of the data subject to be notified that his personal data is being processed. The conditions giving rise to the exceptions must then be satisfied. An example of an exception to the non-disclosure provisions would be where the disclosure is to prevent crime or to detect crime or to prosecute offenders. An example of an exception to the subject information provisions is where notification would prejudice the security of the health, safety or welfare of workers.

aa) Corollary Conditions

Where the exceptions do not apply, a number of alternative conditions have to be met before the data can be said to be 'fairly and lawfully' processed in line with the Principles. In the present context, those conditions are that the 'data subject' has given consent or where it is necessary for the Data Controller to comply with a non-contractual legal obligation or where it is necessary for the legitimate interests pursued by the Data Controller. Given a relatively high threshold to satisfy the concept of 'necessary' then the 'consent' condition is most commonly encountered in practice. Further, processing will not be 'fair and lawful' unless the Data Subject is notified that the processing is taking place. There is no need to give notification if it would either be disproportionate or disclosure is necessary to comply with a legal obligation of the Data Controller. In addition to these considerations, the processing has to be for one or more specified and lawful purposes and the processing must not be 'excessive'. The principles also make it clear that technical and organisational steps must be taken to safeguard against the loss, destruction or unlawful processing of data and that the data shall not be transferred to a country outside the EEA unless equivalent levels of protection are provided as those conferred by the Act. Consideration therefore has to be given to the use of appropriate technology and technology providers.

bb) Scope of the Exceptions

As mentioned, there are exceptions to the duty to comply with the 'non-disclosure' provisions where the data is being processed for the detection or prevention of crime. There is also an exemption to the 'subject information' provisions where the processing would prejudice the discharge of the Data Controller's functions to protect the public against dishonesty, improper conduct or financial loss. These exceptions do not have general

application to routine commercial litigation but may cover some contexts. The exception under s. 35 of the Act only extends to the 'non-disclosure' provisions. The circumstances in which this exception arises are the most apposite to the present context. They are where the disclosure is required by a court order, enactment or rule of law or where disclosure is 'necessary' in connection with prospective of actual legal proceedings or for obtaining legal advice or otherwise where it is necessary to establish, exercise, or defend legal rights. It can be seen from this complex interplay of principles and exceptions that in the absence of 'consent' and in most cases notification, the collecting, reviewing and disclosing data in the context of litigation could amount to a breach of a duty to comply with principles or at least there would be minimal certainty as to whether the principles have been complied with or not.

c) Concept of Consent

Consent is a concept that has generally caused little difficulty in the U.K. but issues related to the "quality" of consent and its vulnerability to withdrawal have created more difficulty in other parts of the EU, notably France. Whilst in the context of disclosure in litigation a combination of the s. 35 exception and the derogation from the requirement to give notice where disclosure is necessary to comply with a legal obligation may mean that notice is not required, it is nevertheless common practice for organisations to attempt to satisfy the notification requirement through generic notices in employment policies and on other official documentation. Whilst technically these attempts may not achieve strict compliance, for the reasons stated earlier this is unlikely to give rise to any problems with admitting the evidence in court. If data is processed otherwise than in accordance with the terms of the Act the Data Controller may be censured, but in most civil cases (and probably in most criminal cases) the judicial discretion to exclude unlawfully obtained evidence is very unlikely to mean that the personal data will not be admissible in the litigation itself.

7. Sanctions in England

Where there are English proceedings and the personal data is located in the U.K., it is very unlikely that the duties imposed by the U.K. Data Protection Act will prevent the data from being tendered in evidence in the proceedings. If the Act is not complied with, the data is still likely to admissible. Suppose in a U.K. litigation case where the U.K. Data Protection Act applies, some of the data to be disclosed is controlled by a party to the litigation in Germany. What happens if because of the application of the German data protection rules, the litigant cannot produce the data it controls? The approach of the English courts is illustrated in the case of *CMCS Common Market Commercial Services AVV v. Taylor [2011] EWHC 324 (Ch)*. In this case there was an issue as to the ownership of a company that was claiming possession of a property. The alleged ultimate owner of the company was joined as a party to the proceedings and was ordered to disclose documents relating to his ownership. The alleged ultimate owner was based in Switzerland and did not give full disclosure on the basis that Swiss secrecy laws obliged him not to. The alleged ultimate owner's refusal to comply with a court order for full disclosure led to him being barred from continuing to take part in the case. Whilst the case is directly about wasted costs and solicitors' misconduct, it is a useful example of the fact that a litigant who is unable to give full disclosure due to the application of non-U.K. laws (including for example because the data is in Germany and German law will not release it), could ultimately be barred from continuing his case. The remedy of debarring a litigant is one of last resort and is only appropriate where the failure to give disclosure cannot be dealt with either by the drawing of adverse inferences against the non-compliant party or otherwise where justice cannot be done.

Where the documents are needed for U.K. proceedings but located outside the U.K. in a country that will not, for data protection reasons, permit the lawful disclosure of the personal data, the Data Controller will have to weigh up the relative merits and demerits of sanctions in the U.K. proceedings vs. sanctions under the law of the country where the data protection rules do not permit the release of the data. The power to impose sanctions for non-disclosure may include the striking out of claims, costs awards, the drawing of adverse inferences or a contempt of court. The penalties for non-compliance with data protection laws may include heavy fines or imprisonment in some countries. When it comes to penalties and enforcement in the U.K., from 6 April 2010 the Information Commissioner's Office has been able to impose penalties of up to £500,000 for serious breaches of the Data Protection Act[14].

II. E-Discovery in Germany – An Example of the Position in Europe

In comparison to the U.S. or U.K. most European countries do not have discovery procedures in place. Nevertheless it may be the case that a discovery or disclosure obligation that initiates in the U.S. or the U.K. includes documents that are in the possession and control of companies located in one of these European countries. Hence, companies based in Germany or in other parts of Europe[15] might be faced with such e-discovery requests to produce ESI.[16] This is especially the case if, for example, such companies operate in the U.S. or England themselves (for example, by 'doing business' or establishing 'minimum contacts') or if they are subsidiaries of American corporate groups due to the 'alter ego theory'. According to the 'alter ego theory' a plaintiff seeking to pierce the veil of limited liability must prove that the subsidiary in question and the corporate group do not act as if they were a separate legal entity. Without such separateness a court may rule that the subsidiary and the group are one and the same. As a result the subsidiary will have unlimited liability for all of the group's disclosure requirements.

1. Enforceability of E-Discovery Requests under the Hague Convention

It is the common belief of many U.S. lawyers and judges that foreign courts may be competent to impose discov-

14 Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010. *See www.ico.gov.uk*.

15 *See* The Sedona Conference, International Overview of Discovery, Data Privacy and Disclosure Requirements, September 2009, for an overview of other jurisdictions.

16 *See Burianski/Reindl*, SchiedsVZ 2010, 187 et seq. on E-Discovery in International Arbitration.

ery obligations on companies located in European countries like Germany or France directly. It is not, however, clear whether such formal e-discovery production requests will in fact be successful due to procedural obstacles such as those set out in the *Hague Convention on the Taking of Evidence Abroad*.[17] The Hague Convention is a treaty signed in 1970 by e.g. the U.S. and a number of other nations. Article 23 of the Hague Convention sets forth a uniform procedure for the issuance of letters of request.[18] However, among other states in the European Union, 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.[19] Hence, litigants from the U.S. or England could not impose any direct enforceable obligation of assistance on German companies under the Hague Convention.

American courts and attorneys, however, do not always seem to regard the stipulations contained in the Hague Convention as authoritative. For example, in the breach of contract case *Accessdata Corp. v. Alste Techs. GmbH*[20], 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.' 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 it 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.'[21] In a U.S. case involving a French litigant, *Strauss v. Credit Lyonnais, S.A.*[22], a magistrate judge for the Eastern District of New York upheld a previous order which ordered disclosure of documents from a French bank in relation to a terrorist attack in Israel. The defendant sought a protective order against sanctions for failing to discover documents 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 contention that violation of the Hague Convention would result in criminal sanctions, the Court cited the Restatement (Third) of Foreign Relations Law of the United States, § 442, which sets out five factors to consider regarding the disclosure of foreign documents that are relevant to U.S. disputes. Based on these factors, the Court again denied the defendant's motion.[23] Such cases have been arising with increasing frequency. The Strauss case echoed *Enron v. J.P.Morgan Securities, Inc,* where the Court ordered production of documents located in France, finding that the French blocking statute[24]was not a sufficient bar to disclosure[25]. Similarly, in *Reino de Espana v. American Bureau of Shipping,* the Court held that Spain's privacy laws cannot exempt materials from discovery since those laws were not applicable in the U.S[26]. As a result in most cases the discovery obligation works at least indirectly because most companies adhere to court orders due to the fear of facing sanctions or because they may have an interest in the process.

Importantly, a significant reason why discovery requests are so successful despite European privacy laws is that the responding party fails to demonstrate that providing personal information would be a breach of fundamental privacy laws. Therefore, it is necessarily required to submit precisely the facts about the foreign privacy law and explain the court in detail the conflict. Shira A. Scheindlin, judge for the Southern District Court of New York, recently said at an event of the Georgetown Advanced E-Discovery Institute that it is the job of lawyers to educate the judge, problem is that many U.S. judges have no experience in foreign law and international issues. The parties, therefore, need to encourage U.S. courts to take into consideration and respect foreign privacy law. U.S. discovery of foreign materials has not proven limitless, however. In *Linde v. Arab Bank,* the Court applied the same balancing test that was applied in *Strauss*, and in this case it found that since the majority of the factors weighed in favour of the party opposing discovery, the Israeli confidentiality laws could serve as a barrier to discovery[27].

2. Data Privacy

In contrast to U.S. data protection laws, the data protection laws in Europe protect the individual against his rights to privacy being impaired through the handling of

17 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).

18 The letters of request are petitions from a court in one nation to a designated central authority in another country requesting assistance from that authority in obtaining information that is located within the central authority's borders. An approved letter of request permits the transfer and processing of data.

19 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.

20 *Accessdata Corp. v. Alste Techs. GmbH*, 2010 U.S. Dist. LEXIS 4566 (D. Utah Jan. 21, 2010).

21 *Id.* at 544 n. 29.

22 249 F.R.D. 429 (E.D.N.Y. 2008).

23 These factors which U.S. courts consider in deciding whether to issue an order directing production of information located outside the U.S. 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 U.S.; (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 U.S., or compliance with the request would undermine important interests of the state where the information is located.

24 Countries may enact blocking statutes specifically intended to block international data transmission, even if the collection, processing or other use of information would be permissible within the country's borders. See for example, French Penal Law 80-538 which provides: Subject to international treaties or agreements and laws and regulations in force, it is forbidden for any person to request, seek or communicate, in writing, orally or in any other form, documents or information of an economic, commercial, industrial, financial or technical nature leading to the constitution of evidence with a view to foreign judicial or administrative procedures or in the context of such procedures.'

25 *Enron v. J.P.Morgan Securities, Inc.*, No. 01-16034 (Bankr. S. D. N.Y. July 18, 2007).

26 *Reino de Espana v. American Bureau of Shipping*, 2006 WL 3208579 (S.D.N.Y. Nov. 3, 2006).

27 *Linde v. Arab Bank*, 2009 WL 1456573 (E.D.N.Y. May 22, 2009).

his personal data.[28] Under the compulsory requirements of European Union data protection laws, the disclosure and transfer of personal data is generally prohibited[29]. In addition, European Union and German privacy laws are inspired by the principles of data avoidance and data economy, i.e. as little personal data as possible should be collected, processed and used.[30] This gives the individual the right to control any third party access to his personal data and this is recognised – at least under German law – as a high ranking, fundamental and even constitutional right and principle. It follows that under German law, the collection, processing and disclosure of data collected in the context of an e-discovery exercise is subject to the German Data Protection Act[31]. Therefore, a data controller is under full responsibility to collect, process and use (which includes the production and transfer of) personal data contained in electronic files in accordance with principles set out in the data protection law. Violations of the German Data Protection Act may be prosecuted as administrative or criminal offences (according to Section 43 German Data Protection Act the former are punishable by fines and the latter, according to Section 44, paragraph 1 of the German Data Protection Act, even by imprisonment for up to two years).[32] In the French case *In re Advocat Christopher X, Cour de Cassation*[33] the French Supreme Court affirmed a criminal conviction under France's Blocking Statute[34]. This was the first reported conviction under this statute. The case arose from a discovery order in *Straus v. Credit Lyonnais*[35]. In addition, the provisions of the German Data Protection Act may also be enforced by the individual data subjects (Section 34 German Data Protection Act) as well as the competent data protection authorities (Section 38 German Data Protection Act).

This means that the collection, production and transfer of personal data can only be carried out if permitted by the German Data Protection Act or any other German legal provision or if the data subject has explicitly consented. Only exceptionally, e-discovery exercises might be permitted without fulfilling these categories. However, this exemption may only be used very restrictively in order to comply with the principle that under German data protection law any collection, processing or use of personal data is basically prohibited unless explicitly allowed.[36] Furthermore, as regards personal data from employees, this is only possible under the strict regulations of Sections 28 and 32 German Data Protection Act. Under Section 32, the processing of personal data of current employees and also former staff is only permitted under certain, very limited circumstances.[37] Furthermore, the collection and storage of data may only 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.[38] This means that the respective data controller (the company gathering ESI) 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. Therefore, before producing emails that may contain personal data the 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. Even if the collection and production of electronic data has taken place, the subsequent transfer of the relevant ESI abroad may also be problematic. Under Section 4b, paragraph 2 of the German Data Protection 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 to which the data is to be transferred. It is important to note that under German law the level of data protection existing in Germany is not considered to be the same outside the EU/EEA.[39]

It follows that the broad extent of data transfers often required under the American process of e-discovery is not compatible with German or European Union data protection law. The fact that many employees at companies are permitted to use email and Internet for their own personal use may also render the situation more complicated as in such situations, the employer is treated as a provider of telecommunication services under the German Telecommunications Act. In these situations, the company is obliged to protect the secrecy of telecommunications. Similar to the German data Protection Act, the German Telecommunication Act contains special requirements for the cross-border transfer of personal data. Those requirements apply to any cross-border transfer, even within the EU. Therefore the transfer of ESI to countries like England might be problematic as well. It is important not to forget that the Works Council (if any should exist within the relevant German companies) also has certain rights of determination in connection with the use of emails and Internet access of the employees under the Works Constitution Act. In most cases, the potential collection and transfer of such data to the U.S. would, therefore, have to be first discussed with the relevant Works Council at an early stage of the e-discovery exercise.

28 *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.*

29 Article 7 of Directive 94/46/EC.

30 Section 3 of the German Data Protection Act.

31 The German Federal Data Protection Act (Bundesdatenschutzgesetz). *See Rath/Klug*, K&R 2008, 596 (598).

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

33 Appeal No.: 07-83228 (Supreme Court, France, Dec. 12, 2007).

34 French Penal Law 80-538.

35 242 F.R.D. 199 (E).

36 *See Simitis*, BDSG, § 28 no. 133.

37 Section 32, paragraph 1of the German Data Protection Act currently 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.'

38 Section 28, paragraph 1, No. 2 of the German Data Protection 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. insofar 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, [...].

39 Furthermore, in Germany, such transferred data could only be used in the context of legal proceedings. In the U.S., however, documents filed as part of public legal actions are generally available to the public. This would also conflict with the requirements of Sections 4b and 4c of the German Data Protection Act and of Article 25 and 26 of Directive 94/46/EC.

III. An Irreconcilable Difference?

For all the reasons discussed above, European data protection laws and the rules of discovery/disclosure in the U.S. and U.K. seem to be incompatible. Different approaches to the predicament haven been taken around the globe. Against a backdrop of a complex set of laws, diversity in these laws from country to country and increasing penalties for not complying with them, how can companies go about transferring data when responding to discovery requests for information in a legally compliant manner?

1. Guidance from European Data Protection Bodies

In Europe, the 'Article 29 Data Protection Working Party'[40]has adopted the 'Working Document 1/2009 on pre-trial discovery for cross-border civil litigation (WP 158)'[41], which provides guidance to data controllers subject to European Union law on 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 that this must be well balanced with the rights of the individual whose personal data is being sought.[42] The Working Party acknowledges the need for reconciling the requirements of the U.S. litigation rules and the European Union data protection provisions, but also confirms that there must be compliance with applicable data protection requirements. Therefore, 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 implemented into German data protection law as set out above).

In essence, the Working Party as well as the German equivalent, the so-called '*Düsseldorfer Kreis*', hold that an obligation imposed by a foreign legal statute or regulation (such as Rule 26 of 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 that from a European Union perspective that there is an 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 which is objectively relevant to the issues being litigated. Also, where it is possible 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.[43] The Working Party also offers some practical guidance on how to handle personal data in a litigation context and states the following: "As a first step controllers should restrict disclosure if possible to anonymised or at least pseudonymised data. After filtering ("culling") the irrelevant data – possibly by a trusted third party in the European Union – a much more limited set of personal data may be disclosed as a second step."[44]

Besides the German data protection authorities, also the French Data Protection Authority (Commission nationale de l'informatique et des libertés)('CNIL') has issued guidance to help French companies comply with data protection obligations after receiving pre-trial discovery requests from the US.[45] Data located in France can be directly transferred to the US for discovery purposes if certain conditions are met:

- The data transfer takes place only once.
- The data transfer contains a 'non-massive' amount of personal data.
- There are safeguards in place to protection the data.[46]

The recommendations also list methods companies can use to comply with data protection principles in cross-border litigation. CNIL has suggested that data controllers use electronic filtering systems in order to check on the proportionality and quality of the data. If data cannot be anonymised, categories of data to be transferred must be limited to a data subject's name, job title, address, telephone number and data directly related to the litigation. Personal data should be kept secure and access to it should be tracked electronically. It should not be retained for longer than is needed for the litigation.

2. Guidance from "The Sedona Conference"

Engaged in an active dialogue with the Article 29 Working Party and the national data protection authorities,

40 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.*

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

42 The Working Party considered the effects of the Restatement (Third) of Foreign Law of the United States no. 442 and the various decisions 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.

43 The 'Sedona Principles Addressing Electronic Document Production' published by the 'Sedona Conference' provide some additional guidance on the handling of ESI in the context of an e-discovery exercise taking place in the U.S A copy of the Sedona Principles is available for download at the Sedona Conference's website, *www.thesedonaconference.org. 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.*

44 See Working Document 1/2009 on pre-trial discovery for cross-border civil litigation (WP 158), page 10.

45 The CNIL guidelines on discovery are available in French at *http://op.bna.com/pl.nsf/r?Open=byul-7v5nrv.* The summary provided can be found in an article by Lisa Nuch Venbrux in the Privacy and Security Law Report of 24 August 2009 available at *http://www.hunton.com/files/tbl_s10News%5CFileUpload44%5C16570%5CBNA_FrenchData Protection_8.09.pdf.*

46 Such transfers can be justified by an exception under Article 69 of the data protection act, Act n°78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties (Amended by the Act of 6 August 2004 relating to the protection of individuals with regard to the processing of personal data).

the American organisation "The Sedona Conference" has also published some suggestions to manage the legal challenges of cross-border e-Discovery.[47] In view of the complexities and conflicts on cross-border litigation, particularly related to the international management, discovery and disclosure of electronically stored information, The Sedona Conference 2005 launched "Working Group 6" to address issues and develop some practical guides. In December 2011, Working Group 6 drafted a framework to provide guidance to American courts and international litigants on how to handle the conflict between stringent European data privacy law and liberal American discovery and preservation rules. The so called "International Principles on Discovery, Disclosure & Data Protection" were written by an international group of experts in the field of data privacy law and cross-border disputes. It is a non-binding recommendation, including best practice instructions for cross-border litigation. Basic idea of the principles is the theme of cooperation. The Sedona Conference is convinced that potential conflicts of law concerning discovery often can be avoided or minimized just through extensive cooperation between the parties, particularly through confidentiality agreements and protective orders. As far as possible the plaintiff and defendant, in the phase of pre-trial discovery (the requesting and responding party), should try to reach agreements that allow them to commit relevant information in compliance with EU laws.

Thereby the International Principles propose a three-stage approach for parties to prevent conflicts: (1) a stipulation by the parties or court order to ensure special protections for data that is subject to data protection laws; (2) a scheduling court order that guarantees a phased discovery process (with enough time to implement data protection processes and examine if relevant information can be gathered from sources that are not covered by data protection laws); (3) a detailed legitimization plan by the parties to achieve the best possible legal compliance with European data protection law and U.S. discovery rules[48]. This overarching idea of cooperation and collaboration is based on six general principles, the Sedona Conference suggests as guidance for the parties during the discovery phase of litigation. They are as follows:

(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 any party's 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."[49]

3. Practical Experiences

a) U.S.: Balancing Test

In determining whether to order a party to produce documents in contravention of the laws of a foreign country, U.S. courts may employ a balancing test as they did in *Gucci Am., Inc. v. Weixing* L[50]i and *Strauss v. Credit Lyonnais*[51]. Courts in New York, for example, balance the following five factors: (i) the importance to the investigation or litigation of the documents or other information requested; (ii) the degree of specificity of the request; (iii) whether the information originated in the U.S.; (iv) the availability of alternative means of securing the information; and (v) the extent to which non-compliance with the request would undermine important interests of the U.S., or compliance with the request would undermine important interests of the state where the information is located[52].

b) The German Perspective

Although parties may require the assistance of the court to resolve irreconcilable differences, practice at some firms indicates that alternative arrangements can be agreed to among the parties. One example of such cooperation is when cross-border litigants enter a data transfer agreement, which governs the foreign party's production of materials, such as ESI. Consider the following hypothetical scenario: A U.S. litigant sends a document request to its German adversary, which calls for the production of all emails for certain individuals for a five year period. In this case, the German adversary may refuse to produce such emails due to German data protection laws. A helpful solution to this problem, that

47 Founded in 1997, The Sedona Conference is a "non-profit, research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation and intellectual property rights" (about The Sedona Conference: *https://thesedonaconference.org/aboutus*).

48 As appendix to the Principles, the publication included a model protective order and a Cross-Border Data Safeguarding Process and Transfer Protocol (as basis for a legitimization plan).

49 International Principles on Discovery, Disclosure & Data Protection: Best Practices, Recommendations & Principles for Addressing the Preservation Discovery of Protected Data in U.S. Litigation, European Union Edition, December 2011.

50 2011 U.S. Dist. LEXIS 97814, at *15-16 (S.D.N.Y. Aug. 23, 2011).

51 249 F.R.D. 429, 438 (E.D.N.Y. 2008).

52 *See Gucci Am., Inc.*, 2011 U.S. Dist. LEXIS 97814, at *15-16. *See* Restatement (Third) Foreign Relations Law § 442(1)(c).

would not involve going to the judge, would be to rely on a data transfer agreement. Pursuant to that agreement, the German adversary could agree to produce the requested documents in a redacted format; any information – such as names or job titles – contained in the emails could be substituted with generic information. Instead of listing 'Joe Smith' as the email's author and his title of 'Compliance Analyst' as Joe Smith's title, the redacted format would list 'Individual 1' and 'Low Level Employee.' Creative and alternative solutions such as this hypothetical agreement can be tailored to meet different country's data protection rules.

c) The U.K. Perspective

From the U.K. perspective, there are three possibilities when it comes to cross-border data transfers:

aa) A Transfer to the U.S.

A transfer to the U.S. does not give rise to any insoluble problem in practice. The U.K. has no blocking statutes and there are exceptions (contained in schedule 4 to the UK Data Protection Act) to the 'no transfer' rule which are workable in most cases. As noted above, the Data Protection Act in the U.K. forbids the transfer of personal data out of the EEA in circumstances where there is no equivalent protection in the recipient state to that provided by the Act. Therefore, in relation to a transfer from the U.K. to, for example, the U.S. (where data privacy law is generally less stringent than that of the 1998 Act) the solution is to structure a contractual agreement between the 'exporting' Data Controller and the recipient organization to guarantee equivalent protection to that provided by the Act.

In circumstances where it is not possible to create such a contract, the solution is to obtain an order from the English Court. In Re *Madoff Securities International Limited*[53] the liquidators of the English company wanted to transfer personal data to the U.S. There was an inadequate level of data protection inherent in the transfer.

The Court expressly referred to s.4 of the 1998 Act, '*personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subject in relation to the processing of personal data.*' The Court was satisfied in the circumstances of the case that the exception to this rule in schedule 4 paragraph 4(1) of the Act (the transfer is necessary for reasons of substantial public interest) applied to enable the transfer of the information to unravel the alleged fraud and what had happened to the assets. The Court was also satisfied that the other exceptions in schedule 4 (the transfer is necessary for the purpose of or in connection with any legal proceedings (including prospective legal proceedings)) was satisfied as indeed was the exception that the transfer is otherwise necessary for the purpose of establishing, exercising or defending legal rights. Interestingly, the court thought that it was likely that the third exemption (the transfer is necessary for the purpose of obtaining legal advice) was also satisfied but made no finding to that effect.

53 [2009] All ER (D) 31.

bb) A Transfer to Europe

A transfer from the U.K. to Europe presents no problem since the restrictions of the Act do not apply.

cc) A Transfer from Europe

A transfer from Europe to the U.K. or from Europe to the U.S. when viewed from the perspective of English law should be as workable as a transfer from the U.K. to the U.S. In practice, however, the application of the local law in the European state (other than the U.K.) may well conflict with the approach of the U.K. law and substantially complicate the position. The problem would seem to be most acute in the case of proposed transfers to the U.S. from non-U.K. EU states.

4. The Use of Technology to Overcome Data Protection Obstacles

Apart from the legal mechanisms which can be relied upon, technology can also be effectively employed to process data for discovery purposes and reduce the risk of breaching data protection and privacy laws. Electronic filtering is often used to ensure that large data sets are reduced so that it can be argued that the processing of personal data is proportionate and searching and selection tools can also be used to isolate personal and sensitive data and allow it to be handled carefully. From the perspective of a provider of e-discovery technology and services, a variety of approaches to addressing data protection laws are taken by organizations and their appointed legal advisors not just within Europe but also within specific countries.

a) On-Premise Solution

At one end of the spectrum an organization can use it's own IT infrastructure to process documents at its own premises, filter them to identify relevant documents and make them available for review to a legal team also situated within the organization. In this way all possible data transfers can be prevented and controlled by the company as it is possible to disable all access to the data via the Internet. This approach tends to be more costly than others but is used to minimize any contraventions of data transfer related laws and where the data is of a particularly sensitive nature

There are also mobile data processing facilities which can be set up on certain cases, bearing in mind that large volumes of data are best handled in a data centre.

b) Intra-Country Solution

Another option is to make use of an IT infrastructure located in the same country in which the data was originally collected (as opposed to an 'on-premise' solution as described above) to process the data and make it available for review. Organizations sometimes insist that those with the ability to access and review the documents are located in the same country as the data or are at least within the EU. Others allow the review team to be situated outside of the EU including in the U.S. and to access the data via the Internet. A key question, and one requiring local legal advice, is whether the mere act of viewing the data in another country is considered to be a 'transfer' of personal data prohibited by data protection laws.

c) Centralised Data Processing Centre

A third option is to make use of a centralised data processing centre in Europe to process and filter the data and make it available for review. A key question here is whether the transfer of data from the country where it is collected to a data centre in the U.K., for example, is lawful. Generally speaking intra-country data transfers in the EU present less challenges than transfers of data from Europe to the U.S. for processing, but this is not always the case and local legal advice is again recommended. The same considerations in relation to the review of the data discussed above also apply in this scenario.

When technology is used to provide filtering (whether this is done on-site, in the country, or at a central data processing centre in Europe) keyword searching is applied to the data. This can be done on an 'inclusive' basis, i.e., including documents that contain one or more words from a list and on an 'exclusive' basis, i.e., excluding documents that contain one or more words. Whilst this approach is not foolproof and it is possible, indeed likely that personal data will pass through these filters, the process at least demonstrates to the relevant authorities that rigorous attempts have been made to exclude personal data and to identify the data strictly relevant to the issues at stake, as required by the Article 29 Working Party in its opinions on pre-trial discovery for cross-border civil litigation.

Self selection of data is also employed, either in isolation or in conjunction with other options in order to remove personal data. In its most straightforward form this entails asking individuals to either identify documents which are responsive to a specific discovery request or obligation or to identify private documents and emails. This can be done either within the source application (e.g. within Microsoft Outlook) or within a first pass document review tool. By involving the employee in this process it is likely that personal documents will be excluded from the subsequent data transfer. However, relying on the employee to select responsive or relevant documents or to have any input into the document identification is clearly not without its dangers as in certain situations this could be used as an opportunity to remove key documents. The neutrality of technological filtering approach is therefore lost. Organisations have also been known to set up proactive internal procedures in which employees are instructed to mark any private emails, by for example, using certain keywords in the subject line. Automated searches are then used to exclude these documents from data transfers. In this way, the onus is on the employee to identify personal documents.

Commonly, where data needs to be transferred to the U.S. from an organisation in continental Europe, it is first transferred to a data processing centre in Europe, for example the U.K., where it is processed, filtered and hosted.

A legal team will then carry out a 'first pass' document review in which it identifies documents that are likely to be relevant and excludes personal data by using a combination of keyword searching and manual review. Redactions can also be used in order to hide personal information where necessary. The resultant 'anonymised' data set is then exported to another database in which a full and more comprehensive document review related to the issues in the case is carried out. This database can be hosted in the U.K. or in the U.S. as required. By processing and searching across the data in Europe first a party can show that steps have been taken to limit the data transferred to that which is strictly necessary to the case. This is in line with the Article 29 Working Party requirements that efforts should be made to restrict the transfer of personal data as much as possible and that only data which is relevant to the issues being litigated should be transferred.

IV. Conclusion

Cross-border litigation is growing in the global economy and complexity in cross-border cases (whether U.S.-led or not) results from legal variances in different jurisdictions. Companies in Europe are no longer only subject to European Union rules and regulations and an inevitable conflict arises between discovery obligations on the one hand and privacy rights on the other. Apart from that, there are significant differences in the maturity of attitudes towards e-discovery in different jurisdictions and the existence or scope of the discovery obligation varies from one jurisdiction to the next, particularly as between the common law jurisdictions and the non-common law countries of the EU. Despite the Data Protection Directive (and in the future the Data Protection Regulation) applying across Europe, other domestic laws and the differing interpretations of the Directive create something of a mine field when it comes to the "processing" of personal data, including its movement across certain legal jurisdictions. The Article 29 Data Protection Working Party and The Sedona Conference recognize the difficulties that arise when cross-border data transfers need to take place in the context of pre-trial discovery but do not offer a simple legal solution, no doubt because no such simple solution is yet available. The Working Party and The Sedona Conference have nevertheless provided useful practical guidance on how technology and electronic filtering systems can be used to restrict the disclosure of personal data.

In terms of the future, a radical reform of the European Data Protection Directive is planned. At present, the European Commission is going through a review process of the European data protection framework.[54] Key changes in the reform are the introduction of a single set of rules on data protection valid across the EU; some new privacy principles such as data minimization and accountability, new data controller responsibilities; a requirement to report data breaches as soon as possible; stronger enforcement powers and fines and the application of the EU rules if personal data is handled abroad by companies that are active in the EU market and offer their services to EU citizens.

However, the proposed EU General Data Protection Regulation will not provide a solution to the conflict between privacy and discovery.[55] According to Article 17 of the draft of the EU Regulation any person

54 *See* European Commission: Justice, *Review of the Data Protection Legal Framework*, available at *http://ec.europa.eu/justice/policies/privacy/review/index_en.htm* (last accessed 20 January, 2012).

55 The draft of the General Data Protection Regulation can be found at *http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf*.

should have the right to have personal data concerning them rectified and a 'right to be forgotten' where the retention of such data is not in compliance with this Regulation. It is expected that this provision will fuel the flames of conflict regarding e-discovery. In addition the Regulation repeats the derogation in the Directive which states that a transfer of personal data to a third country with inappropriate safeguards may by way of exception take place if the transfer is necessary for the defence of legal claims[56]. From a German perspective, the Düsseldorfer Kreis has already held that pre-trial discovery does not fall into the scope of this derogation because pre-trial discovery does not serve as defence. It remains to be seen if U.S. courts agree with this approach. Rather, the new Regulation is likely to see the requirement for consent to transfers of personal data across borders to be strengthened to 'explicit consent' as is the case under U.K. data protection law. Further rules are expected in relation to transfers of data out of the EEA but within a corporate group[57]. These reforms are not likely to lessen the difficulties presently being experienced. Most notable of all the proposed reform is the possibility of fines of 2 % of global turnover in relation to serious breaches of the Directive. If anything the risks and difficulties are set to increase. Local legal advice is therefore essential to ensure compliance with the different procedural rules and privacy laws that come into play, to avoid sanctions for non-compliance and to ensure the litigation is not prejudiced. Besides it has proven to be helpful to present to the competent common law court and/or attorney a legal opinion setting out the imperative rules of European privacy laws and showing that the broad e-discovery requests are likely to be in violation of law. In essence, at least where there is a true conflict of laws such as between American law and that of a foreign jurisdiction, applicable conflict of law rules will require the Court to conduct a comity analysis.[58] There is no silver bullet available that will cut through the labyrinth of complex laws that must be navigated in order to devise an effective and pragmatic approach to cross-border data transfers in international litigation. It is vital that organisations not only have a strong knowledge of the current legal and IT landscape but also of technological options available to facilitate lawful data processing and cross-border data transfers and to reduce the risk of breaching privacy laws. It is only by keeping a close eye on the way both of these constantly evolve that businesses can ensure that they adopt appropriate procedures and keep risks in check.

56 See Article 44 paragraph 2 lit. e of the Regulation and of Article 27 paragraph 1 lit. D of Directive 94/46/EC.

57 One of the most significant changes in the revised framework is the revision to the Binding Corporate Rules, which will have a statutory basis. Article 40 of the Proposed General Data Protection Regulation ('Regulation') will streamline the BCR approval process and make BCR available to data processors as well as data controllers.

58 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 Communication Corp. v. Societe Generale (In re Maxwell Communication Corp.)*, 93 F.3d 1036, 1050 (2d Cir. 1996); *Hilton v. Guyot*, 159 U.S. 113 (1895).

About the Authors

Karl Geercken is the chair of the Litigation and Trial Practice Team in New York at Alston & Bird. His practice focuses on complex commercial litigation and arbitration, bankruptcy litigation and products liability defense. Karl has extensive experience in representing international clients, and, in particular, European commercial and governmental entities in sophisticated litigation matters. Karl received his undergraduate degree, magna cum laude, from the University of Rochester in 1987 and his J.D. from The George Washington University National Law Center, where he was a member of the Journal of International Law and Economics. Karl is a member of the American Council on Germany and is also on the board and executive committee of CDS International, Inc., a not-for-profit organization that fosters international professional exchanges.

Kelly Holden is an associate in the New York office of Alston & Bird and a member of the firm's Litigation and Trial Practice Group. Her practice is focused on general commercial litigation. Kelly received her J.D. degree from Boston University School of Law (BUSL) in 2008. While at BUSL, she was the technical editor of the *International Law Journal*. She completed her M.A. degree in international relations in December 2008. Before law school, Kelly attended the University of Michigan, where she received B.A. degrees in English and Arabic/Islamic Studies.

Michael Rath is a German attorney-at-law and a partner at Luther Rechtsanwaltsgesellschaft mbH, Cologne, Germany, with a high specialization in matters relating to information technology (IT), data protection and copyright law. He is a certified expert attorney on IT law and became member of the German Bar in 1999. Michael has gained particular experience in technology-related transactions including outsourcing, licensing and technology transfer. He advises German and international clients including forensic services consultants in e-discovery disputes and internal investigations. Michael often advises on privacy and (IT-) compliance issues and is author of various publications in the IT sector.

Tracey Stretton is a Legal Consultant at Kroll Ontrack in the UK and advises lawyers and corporations on the use of technology in investigations and litigation. Her experience in legal technologies has evolved from exposure to its use as a practicing lawyer and consultant in a variety of international jurisdictions. She speaks regularly at conferences and has written numerous articles on the impact of technology on law and business. She is a contributing author to the book "Electronic Evidence and Discovery – What Every Lawyer Should Know Now", published by the American Bar Association. She has also contributed to the Sweet & Maxwell Encyclopaedia of IT Law on the topic of "The Management of Technology Related Risks."

Mark Surguy is Partner in the Fraud Group of Eversheds LLP specialising in multi-disciplinary, complex and commercially sensitive cases where urgent legal remedies are required and where large volumes of electronic information have to be collected, searched and produced in court. Formerly Head of Fraud at a large international law firm, he centres on advising corporate and institutional victims of fraud and commercial dishonesty, often in a cross-border context.

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, D-82166 Gräfelfing · Print: rewi Druckhaus, Reiner Winters GmbH, Wiesenstr. 11, D-57537 Wissen

Advertisements: Responsible for advertisements is Gaby Joisten from whom a list of current prices can be obtained. Phone +49-221-93738-421 · Fax +49-221-93738-942 · e-mail: anzeigen@otto-schmidt.de

Subscription rates: (Outwith the subscription to the journal COMPUTER UND RECHT) 194,- € per annum (for members of ITechLaw 174,- € 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 (Print) · 2194-4164 (eJournal)