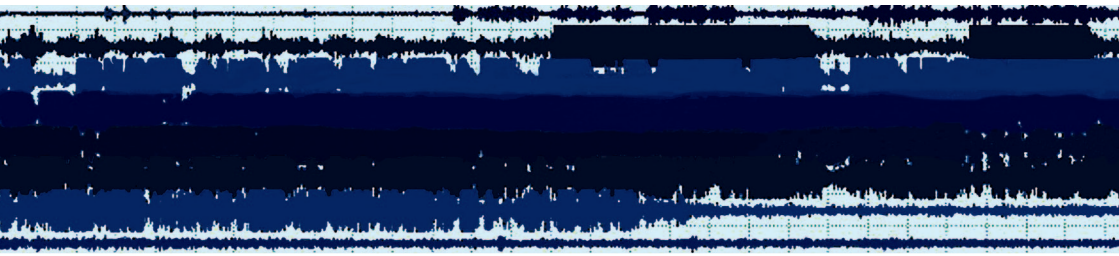
HOUTHOFF BURUMA

US E-DISCOVERY IN THE NETHERLANDS

NOVEMBER 2010



IN-HOUSE COUNSEL PRACTICAL GUIDE

TABLE OF CONTENTS

INTRODUCTION

In 2005 Morgan Stanley was ordered to pay US $1.45 billion after a Florida court instructed the jury that it could presume that a large volume of missing e-mails would have supported the plaintiff's claim against Morgan Stanley if they had been produced in the proceedings. This is certainly every company's worst nightmare. What happened to Morgan Stanley in this case could just as well have happened to any other internationally operating company dragged into proceedings before a US court.

e-Discovery is the pre-trial retrieval and review of electronically stored information for evidentiary purposes in a pending or reasonably anticipated litigation in the US. In the electronic age, disclosure has moved from inspecting and photocopying archived paper files to the rapid searching of vast quantities of information in e-mail archives, shared network folders, voicemail back-up tapes and flash drives. As one American expert has said, "All data is fair game."

The consequences of having to comply with an e-discovery request from an American court can be very costly. A non-American company may likely face conflict-of-laws issues. This guide on e-discovery for in-house counsel in the Netherlands is part of Houthoff Buruma's In-house Counsel Guides Series and will briefly give an overview of how US e-discovery knocks on a Dutch company's door. The guide is meant as supplementary information to our e-Discovery Master Class organised in November 2010, and should not be seen as legal advice but as a practical introduction mapping the landscape of the US e-discovery. Above all else, it appears that the best way to handle the impact of US e-discovery is to be prepared. This guide is meant to be a first step in that direction.

ELEVEN KEY POINTS ON E-DISCOVERY

e-Discovery cannot be ignored. If you fail to produce the requested documents, you will likely lose the case.

Being based in the Netherlands may not protect your company from e-discovery. You do not need to be doing business in the US to be subjected to e-discovery.

e-Discovery involves all electronically stored information coming within the scope of the request, in whatever form and wherever stored, including retrievable information on deleted files.

You may be forced to hand over information even if it is expressly forbidden by Dutch law or EU law.

You will not be the judge of what is considered relevant information.

You need to have a clear and consistent data deletion policy and you need to know when to stop deleting in order to avoid penalties or criminal charges.

Fishing expeditions are not allowed, but in practice e-discovery may come pretty close to that.

Arbitration is not a safeguard against e-discovery.

Even privileged information may be subject to e-discovery.

You may be able to use e-discovery to your own advantage.

Being organised and having a good document management system in place will save you time and money.

E-DISCOVERY IN THE UNITED STATES

Gary DiBianco and Elizabeth Billhimer

The prevalence of electronic communication and devices in the world today ensures that companies engaged in litigation or subject to investigation in the United States will encounter some form of e-discovery. In global business, American litigation and investigations have an increasingly global reach, and e-discovery crosses national borders.

What is e-discovery?

Discovery is designed to allow courts, parties in litigation and regulators in an investigation to determine the truth of matters under dispute. The term "e-discovery" refers to the provision of electronically stored information, sometimes referred to as "ESI." Fundamentally, e-discovery is – except for its form – no different than paper discovery. An important distinguishing factor, however, is the volume of information that often exists in electronic form. In many cases, the volume of electronic information, if printed, would fill many thousand of boxes or even a warehouse.

Applicable rules

The Federal Rules of Civil Procedure govern the discovery process in US federal courts. Four rules in particular are applicable in the electronic discovery context:

Rule 16 (Pretrial Conferences; Scheduling; Management), governs pretrial conferences and scheduling orders. In the electronic discovery context, this rule is designed to alert the court early in the litigation to the need to address discovery involving electronically stored information.

Rule 26 (Duty to Disclose; General Provisions Governing Discovery) requires initial disclosures of all documents and electronically stored information, and tangible things that the disclosing party has in its possession, custody, or control and may use to support its claims or defenses.

Rule 26 also provides some limitations on electronic discovery. It states that "a party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost." Even so, the rule allows the requesting party to formally compel the information, at which time the party withholding the information must demonstrate why the information is not reasonably accessible because of undue burden or cost.

In addition, Rule 26 requires the parties to confer on a discovery plan and submit a proposed plan for discovery to the court. Among other things, the plan must include any issues about disclosure or discovery of electronically stored information, including the form or forms in which it should be produced.

Rule 34 (Producing Documents, Electronically Stored Information, and Tangible Things, or Entering onto Land, for Inspection and Other Purposes) governs requests for production of documents and requires production of "any designated documents or electronically stored information – including writings, drawings, graphs, charts, photographs, sound recordings, images and other data or data compilations – stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form; or any designated tangible things." Thus, "documents" and "electronically stored information" are broadly defined.

Rule 37 (Failure to Make Disclosures or to Cooperate in Discovery; Sanctions) provides that, absent exceptional circumstances, a court may not impose sanctions under the rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.

Importantly, the Federal Rules of Evidence governing privilege can operate to protect certain information from production. The relevant privileges that may apply include attorney-client privilege, attorney work-product privilege, or joint-defense or common-interest privilege.

The attorney-client privilege protects communications between a client and attorney made in confidence for the purpose of seeking or providing legal advice, but only where the privilege has not been waived.

Attorney-work product is an otherwise-discoverable tangible thing that was produced by or for an attorney or consultant, or by or for a client in preparation for litigation. Some fact work-product can still be discoverable if the requesting party can show substantial need and undue hardship in obtaining the information by other means.

The joint-defense privilege protects statements made in the course of a joint-defense, common-interest effort and in furtherance of that effort, but only where the privilege has not been waived. While actual litigation is not necessary, the joint effort must relate to legal claims. A mere joint effort is not sufficient. Also, the joint-defense privilege must be based on an underlying privilege. Hence, a mere sharing of materials with a party

Privileged information can still be discoverable if the requesting party can show substantial need and undue hardship in obtaining the information by other means.

with a common interest does not protect them if they are otherwise unprotected. Finally, because electronic information may be withheld on grounds of privilege, it is necessary to have a review system that allows segregation and redaction of electronically stored privileged materials.

Duty to preserve

If a company is subject to discovery in US federal courts, it has a duty to take reasonable and affirmative steps to identify and preserve potentially relevant information. This duty is triggered not when a lawsuit commences, but when a party "learns or should have learned" of a pending litigation or reasonably anticipates litigation.

Once the duty is triggered, a party must suspend its routine document retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents. See *Zubulake v. UBS Warburg*[1] *:*

"The obligation to retain discoverable materials is an affirmative one; it requires that the agency or corporate officers having notice of discovery obligations communicate those obligations to employees in possession of discoverable materials."

A plaintiff's duty often is triggered before litigation commences, because the plaintiff generally has control of the timing of the litigation. Failure to preserve relevant information in a timely manner can lead to serious sanctions for destruction of evidence.

As set out in the rules, when considering what should be preserved, the term "potentially relevant information" is broadly construed. Thus, consideration should be given not only to obvious forms of relevant information, such as paper documents, e-mails, word processing documents, spreadsheets, and audio and video recordings, but also to other forms of information. Such other information includes, but is not limited to, electronic metadata,[2] other hidden information, inaccessible sources of information, and "non-record" records.

Documents "subject to control"

3

As Rules 26 and 34 make clear, a request for documents is not confined to what is in the responding party's possession, but may include what is under the responding party's "control," including "information reasonably available to the responding party from its employees, agents, or other subject to its control."

Courts have held that documents are in the "control" of a responding party if the party has "the legal right or ability to obtain the documents from another source upon demand." *Mercy Cath. Med. Ctr. v. Thompson*[3].

Afros SPA v. Krauss-Maffei Corp.[4]*:*
"If a party has control over or shares control of documents with a third person, then a court can order production by means of its power over the party litigant."

Engel v. Town of Roseland[5]*:*
"A party has control or custody of a document or thing when he has the legal right to obtain the document, even though in fact he has no copy."

Factors considered in determining "control" include the corporate structure encompassing the entities, the non-party's connection to the transaction, and the degree to which the non-party would receive benefit of any award in the case. See *In re: Global Power Equipment Group, Inc.*[6], in which it was held that a Dutch corporation, a claimant in a US bankruptcy proceeding, exercised control over French sister corporation for purposes of ordering production of documents from French corporation. See also *Flagg v. City of Detroit*[7], in which it was held that possession for purposes of requiring production includes control over the information maintained under a contractual relationship with a non-party service provider. In the case of *In re ATM Fee Antitrust Litigation*[8], it was held that the defendant had access and control over requested electronic data storage and management information which was held by a non-party, wholly-owned subsidiary.

An e-discovery request is not confined to what documents are in the responding party's possession, but may include information under the responding party's "control".

Confidentiality

Certain data protection laws may restrict the collection, processing, reviewing and production of documents in American civil litigation. In addition, blocking statutes in certain countries are designed to prohibit seeking or providing civil discovery in a foreign case unless otherwise authorized by statute or treaty. Even so, US courts will conduct a careful analysis of the relevant foreign laws and statutes at issue, but ultimately may conclude that production of the electronic information is required. See *Linde v. Arab Bank*[9], in which the court denied requests for information from non-party Israel Discount Bank that were subject to Israel bank confidentially laws but granting remaining requests.

The Hague Evidence Convention does not pre-empt the discovery provisions of the Federal Rules of Civil Procedure.

When a US federal court is asked to apply the more stringent procedures in the Hague Evidence Convention[10] to a document request, the courts will conduct an analysis of whether the Federal Rules of Civil Procedure or the Hague Evidence Convention procedures apply. The factors considered in determining how to proceed include: the importance of the documents, the specificity of the request, whether the information originated in the US, the availability of alternative means of securing the information, and the effect of noncompliance on interests of the United States or the state where the information is located. See *In re: Global Power Equipment Group, Inc.*[11], in which the court concluded that risk of prosecution under French Blocking Statute was minimal and granted discovery pursuant to the Federal Rules of Civil Procedure.

Investigations

Although the foregoing rules and concepts apply in the civil context, similar concepts are also applicable if a company receives a request for information or a subpoena from a government regulator or law-enforcement authority. Most importantly, failure to preserve evidence and produce all relevant information in the criminal context could be viewed as separate criminal infractions.

In addition, investigations frequently implicate forensic review of electronic data. Accordingly, particular steps should be taken to ensure the integrity and the "chain of custody" of electronic data.

E-discovery rules also apply to investigations under, for example, Foreign Corrupt Practices Act, the Sherman Antitrust Act, and the Sarbanes-Oxley Act.

Costs and cost-shifting mechanisms

Generally, the party producing electronically stored information bears the cost of production. See *Kemper Mortgage, Inc. v. Russell*[12]*:*

"One of the unexpected costs of using the electronic tool is that it may become costly to abide by one's duty to preserve evidence, but that is not a cost which can be shifted to the opposing party, at least in the absence of a demand for a litigation hold which seeks court enforcement and/or requests for discovery which can limit the amount of information which needs to be preserved."

In some circumstances, courts will consider cost shifting, but only when electronic discovery imposes an "undue burden or expense" on the responding party. In deciding whether to shift costs, courts will consider several factors, as explained in *Zubulake*[13]: "the extent to which the request is specifically tailored to discover relevant information; the availability of such information from other sources; the total cost of production, compared to the amount in controversy; the total cost of production, compared to the resources available to each party; the relative ability of each party to control costs and its incentive to do so; the importance of the issues at stake in the litigation; and the relative benefit to the parties of obtaining the information."

See also *Am. Fast Freight, Inc. v. Nat'l Consolidation & Distribution, Inc.*[14], in which the court considered whether the undue burden or expense outweighs the likely benefit, taking into account "the needs of the case, the amount in controversy, the parties' resources, the importance of the issue at stake, and the importance of the proposed discovery."

In determining whether there is undue delay or cost, courts also will focus on whether the electronically stored information is readily accessible or inaccessible. For example, active or online data (such as data stored on hard drives), near-line data (such as data on magnetic tapes or optical disks), or offline storage or archives (such as removable magnetic tape media for archival use of as disaster recovery), have all been considered readily accessible. On the other hand, courts have deemed data on back-up tapes where the data may be compressed, or data that is erased, fragmented, or damaged as not readily accessible.

In *Universal Del., Inc. v. Comdata Corp.*[15], the court held that a third party had met its burden of showing that electronically stored information was not reasonably accessible because of potentially large production costs and the data

In some circumstances, courts will consider cost shifting between the parties, but only when electronic discovery imposes an "undue burden or expense".

was only in marginally accessible form (back-up tapes). The court ordered the information imaged and produced in a searchable database and evenly distributed the costs between the requesting plaintiffs and the third party based on the inaccessible form of the information. [16]

Conclusion

Electronic devices and communications have greatly simplified the ability to conduct business around the globe in an efficient and effective manner. At the same time, however, it has complicated the process of responding to requests for information during litigation and investigations.

The key to addressing these issues and handling e-discovery requests is to take a proactive stance to management of electronic information in the normal course of business, long before a litigation or investigative need for preserving and producing such information might arise. Creating, implementing, and maintaining a robust records management policy will support future e-discovery efforts and make responding to any discovery requests more manageable.

In the event that preservation of information or "hold" is necessary, companies should inform its officers and employees of the pending litigation and identify for them the kinds of documents considered relevant, in addition to collecting and segregating relevant documents. As one court has noted, "a document retention policy adopted or utilized to justify the destruction of relevant evidence is not a valid document retention policy," and "it follows that implementing such a policy in advance of reasonably foreseeable litigation would not be proper and could constitute spoliation." *Hynix Semiconductor, Inc. v. Rambus, Inc.* [17]

[1] Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 218 (S.D.N.Y. 2003); National Ass'n of Radiation Survivors v. Turnage, 115 F.R.D. 543, 557-558 (N.D. Cal. 1987)

[2] Different rules apply to reviewing metadata of electronic records exchanged among counsel. In the District of Columbia, lawyers are prohibited from reviewing metadata until consulting with the sending lawyer to determine if the metadata includes work product or client confidences. The ABA Model Rules and other states, on the other hand, do not prohibit the review of such metadata.

[3] Mercy Cath. Med. Ctr. v. Thompson , 380 F.3d 142, 160 (3d Cir. 2004)

[4] Afros SPA v. Krauss-Maffei Corp., 113 F.R.D. 127, 129 (D. Del. 1986)

[5] Engel v. Town of Roseland, 2007 WL 2903196, at *3 (N.D. Ind. Oct. 1, 2007)

[6] In re: Global Power Equipment Group Inc., 418 B.R. 833, 844 (D. Del. 2009)

[7] Flagg v. City of Detroit, 252 F.R.D. 346, 354 (E.D. Mich. 2008)

[8] In re ATM Fee Antitrust Litigation, 233 F.R.D. 542, 545 (N.D. Cal. 2005)

[9] Linde v. Arab Bank, 262 F.R.D. 136, 151-52 (E.D.N.Y. 2009)

[10] Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, more commonly referred to as "the Hague Evidence Convention".

[11] In re: Global Power Equipment Group, Inc., 418 B.R. at 850

[12] Kemper Mortgage, Inc. v. Russell, 2006 WL 2319858, *2 (S.D. Ohio, Apr. 18, 2006)

[13] Zubulake, 2003 WL 21087884, at *11

[14] Am. Fast Freight, Inc. v. Nat'l Consolidation & Distribution, Inc., 2007 WL 3357694, *4 (W.D. Wash. No. 7, 2007)

[15] Universal Del., Inc. v. Comdata Corp., 2010 WL 1381225, *7-8 (E.D. Pa. Mar 31, 2010)

[16] Ibid. at *8.

[17] Hynix Semiconductor, Inc. v. Rambus, Inc., 2006 WL 565893, *20 (N.D. Cal. 2006)

THE DUTCH LEGAL PERSPECTIVE ON AMERICAN E-DISCOVERY

Marielle Koppenol-Laforce

How does a non-American company end up getting involved in e-discovery?

2

The most obvious way for a non-American company to get involved in the US e-discovery process is to become involved in litigation in the United States. However, there are more indirect ways. Here are a few examples:

A Dutch company has a branch in the United States and that branch is sued.

A Dutch company merely sells products in the US market, but is sued because of those products. The Dutch company could become involved even if the sales were conducted through a chain of non-affiliated sellers. Or if the sales were not aimed at the US market at all, but the Dutch company failed to make an attempt to make sure they would not be sold on the American market.

A Dutch company is involved in proceedings (pending or contemplated) in the Netherlands or elsewhere, and a party applies under section 1782 of Title 28 of the United States Code for discovery in a U.S. court. This could happen even if the Dutch company is not a party to the proceedings, but for example has only sold products to a party (or assigned contracts or rights) and materials relating to this are in the United States because of the domicile of a director or office.

What discovery is available in the Netherlands under the Hague Evidence Convention?

In principle, when a party is involved in proceedings in either the United States or the Netherlands, the party can rely on the Hague Evidence Convention[1] to attempt to obtain information from another party in a country other than where the case is pending. The Hague Evidence Convention is a multi-party convention that is binding on both the US and the Netherlands.

Under the Hague Evidence Convention, a Dutch court may be requested to order the discovery requested; however, if the request is granted, the discovery will then be conducted in accordance with Dutch law. Even if the Hague Evidence Convention is relied on by an American court, this process cannot lead to the introduction in the Netherlands of a type of discovery beyond what is permitted by Dutch law, including US-style discovery or e-discovery. In particular, the request cannot be executed by a Dutch court beyond the limits of article 843a of the Dutch Code of Civil Procedure ("DCCP").[2]

7

Furthermore, when the Hague Evidence Convention was signed, the Dutch government stated publicly that it would not assist with requests to conduct "fishing expeditions". Regardless, it does

seem that the Dutch courts are increasingly becoming more willing to force parties to produce documents even when these documents are described in the request in a general sense. From a recent questionnaire issued by the Hague Conference on Private International Law , it seems that that, in the case of discovery of electronically stored information ("ESI"), requests from U.S. courts to foreign courts under the Hague Evidence Convention are being executed as if the documents requested were paper documents.

What disclosure is available in Dutch civil procedure?

The Hague Evidence Convention does not prevent a party from gathering evidence by applying directly to the local courts in that other country if those courts permit it. Any party (whether Dutch or international) may attempt to obtain documents, including ESI, through the request process provided for in article 843a of the DCCP.

Dutch or international parties may also obtain documents in proceedings pending in the Netherlands in the usual way, either in an interlocutory motion or as part of the claim or counter claim in the main proceedings.

Whether a discovery request is made under the Hague Evidence Convention or the DCCP, it is made under article 843a of the DCCP.[3] Article 843a states:

1. *Anyone who has records at his disposal or in his custody must allow a person with a legitimate interest in doing so to inspect, to have a copy of, or to have an extract from, those records that pertain to a legal relationship to which he or his legal predecessors are party. "Records" includes information recorded on a data medium.*

2. *If necessary, the court may determine how an inspection is to be conducted or how a copy or extract is to be produced.*

3. *Anyone who by virtue of his office, his profession or his relationship has a duty of confidentiality need not comply with this request if the records are at his disposal or in his custody only for that reason.*

4. *Anyone who has the records at his disposal or in his custody need not comply with this request if there are serious reasons for not doing so and if it may reasonably be assumed that the proper administration of justice is safeguarded even if the information requested is not provided.*

Under this article, a party is required to submit documents and information (whether electronically stored or not) if and in so far as they: relate to a specific legal relationship (tort, contract); are described with sufficient specificity; and are in the possession of the party that is being asked to submit them.

The scope of Dutch discovery is undeniably narrower than what is available in the United States or even the United Kingdom. However, there does seem to be a shift in the Dutch courts to broader disclosure obligations.

In a case involving Fortis, the court ordered the other party to provide all data on a data medium that was in the possession of Mourant and that related to financing structure and/or FCC memorandum, documents relating the public offering, including e-mails, letters, memoranda, notes, advice letters and draft documents.[4] In making this decision, the court probably found it significant that before the Fortis group was split up, the requesting company had itself had possession of these documents or at least had had an undeniable right to them. In another decision, it was held that for discovery to be ordered, it was sufficient if the court could ascertain which documents were being requested and that it was reasonably certain that those documents existed.[5] The requesting party was required to try to describe those documents in as much detail as possible, but in this case that was sufficient.

The latest challenge to the scope of article 843a of the DCCP will most likely be the request submitted in one of the Nigerian pollution suits started against Shell plc.[6] The claimants are a Dutch environmental organisation (Milieudefensie) and a few individuals living in Nigeria. The suit concerns a dispute about oil leakage from a pipeline operated by a joint venture that includes an indirect subsidiary of Shell plc. There are three similar cases pending in the Hague Court. In one of the cases, the court held that it had jurisdiction because the office of Shell plc is in The Hague and because of the connection between the claims made against Shell plc and Shell Petroleum Development Company of Nigeria. The documents submitted to the court by Milieudefensie are available on Milieudefensie's website. The request made under article 843a of the DCCP is extremely broad and includes a request for board minutes, reports and any material connected to the condition of the relevant pipeline in Nigeria. The claimants are also asking for documents showing that Shell had been requiring its Nigerian subsidiary to comply with its environmental policy. For an American lawyer this would not be a particularly broad discovery, but it remains to be seen whether a Dutch court is willing to shift further towards the American civil procedural view of what is discoverable. If and when the request is granted, the second issue will be how to manage it. The Dutch civil procedural system lacks the rules, customs and protections that have developed as part of the US discovery process. This problem especially applies to the vast amount of ESI involved.

Are there any defences against an e-discovery request?

11

If a discovery request is made in the United States (whether in proceedings there or, under section 1782 in title 28 of the United States Code, in connection with proceedings in the Netherlands), there is not much that can be done. The main thing an internationally active company can do to protect itself from an American e-discovery request is to have its systems in order so that the information can be provided at the lowest possible cost.

Experience has shown that informing a US court of the more restricted role of discovery in the Netherlands usually does not prevent a US court from giving the order.

A US court cannot really be persuaded to deny an e-discovery request, even if the request in the United States is a limited one, and the request for documents could have been submitted more expeditiously to the Dutch courts directly.

Nor is it a defence to argue that the form of the evidence is insufficient. A Dutch court has the discretion to accept any form of evidence whatsoever.

As discussed in another article in this guide, sometimes privacy laws can provide a reason for limiting discovery. However, this is not always applicable or effective.

A mechanism that might be employed to limit exposure to the American-style discovery is for parties in international contracts to agree on rules limiting discovery and to insert an appropriate clause in the contract. This would not work against third parties, but it might prevent the other party from starting the discovery process set out in section 1782 of Title 28 of the United States and, if the litigation is taking place in the US, limit the discovery process. Under Dutch law, these agreements are considered to be agreements relating to the burden of proof (*bewijsovereenkomst*) and are allowed.[7]

If sensitive information is involved, this information is commonly protected by obtaining a "protective order" from the American court. However, this order will not have the same effect if the protected information is being used in Dutch litigation. In this event, to obtain the same kind of protection, one would have to file a request to the Dutch court for the Dutch proceedings to be closed to the public (*met gesloten deuren*)[8] and published only in a format in which the names are not stated. Such a request is usually refused in ordinary commercial disputes, but if an American protective order has already

You can ensure with your contract partners that the scope and consequences of e-discovery stays manageable.

been issued, a Dutch court will most likely be more inclined to grant the request. When obtaining a protective order from a US court, it is advisable to have a clause inserted in the order stating that both parties are to cooperate in obtaining the same protection in foreign proceedings.

How can a Dutch company balance US preservation requirements with Dutch practice?

In Dutch civil procedure, there are no specific rules for the preservation of documents and certainly not for the preservation of documents starting at a certain point in time. The discovery and disclosure process common in the US and UK is not known to Dutch law.

This raises the risk that e-mails will be deleted – accidentally or intentionally – at a time at which it is considered to be perfectly legal to do so in Dutch civil procedure, but illegal under the US or UK rules. Not only is it not fully clear to a Dutch company when the company must stop deleting any documents (including ESI) under the applicable US or UK rules, but the Dutch lawyers advising these companies are not even alerted by a notice or letter from the US or UK party that deleting is no longer acceptable.

Ordinarily, any deleting that takes place in the course of normal practice is acceptable, even in the US system, at least up until a certain point in time (see regarding duty to preserve previously in this guide). A company could therefore explore whether some protection could be had from introducing a strictly and frequent deletion routine. Especially if a company has a sensitive research and production programme, it might be worthwhile to introduce a regular deletion routine for e-mails exchanged between employees.

What should be done in the event of attachment (*beslag*) of electronic information?

In Dutch law it is possible for electronic data stored on computer hard disks, servers or other storage devices to be attached pending the outcome of litigation. The procedure of attaching materials that constitute evidence was introduced into the DCC for intellectual property disputes. By not construing this process too narrowly, Dutch courts have accepted that it might be applied in other disputes as well.

In order for an attaching party to obtain something useful, and at the same time for the operations of the attached party not to be disrupted, the court usually imposes certain conditions in the attachment. For example, the order may include the requirement that the attaching party not be allowed to witness the transfer or examine the data itself. The court may order that the data be copied within a short time period. As the bailiff (*deurwaarder*) is not expert in this field, he or she may require that the requesting party consent to the hiring of an ICT expert. Usually the data copied must be held pursuant to a storage agreement between the attaching party, the bailiff and a third party knowledgeable in ICT matters.

A court may lift an attachment if it appears in a summary review that there is no claim. A Dutch court will not be quick to lift an attachment aimed at preserving evidence if the attaching party has an arguable case under article 834a of the DCCP, especially if the attaching party is not entitled to examine the data attached.

What role does good corporate governance play in the e-discovery process?

Good corporate governance plays a major role in handling e-discovery.

First, a company should prepare itself by having strict rules relating to electronic information. We all know that mistakes are usually caused by human error, so to have guidelines in place is not enough. It is useful to have wide-ranging policy that addresses issues like: what may be done during office hours, how to deal with e-mails, how to store e-mails, to whom cc's and bcc's should be sent, and who in the end holds the final agreements.

However, this policy is only useful if someone checks and ensures compliance. To do all that simply in preparation for the unlucky day that e-discovery comes knocking on the door would be rather costly. This is where corporate governance comes in.

A board should at all times be aware of the rights and duties of the company. This means that systems that make it easy to access contracts should be put into place. This should also prevent each salesperson from starting to invent his or her own contractual arrangements. If the company is of a certain size, it cannot do without a document management system. Nowadays, because ICT systems can link huge amounts of information together, a neat system will not just help meet corporate goals, but also save a lot of time when that knock comes on your door.

Good corporate governance also requires having a system that stops employees from not sending e-mails faster than they can think or blurting everything they can think of out in the e-mail. Badly drafted e-mails (often in poor English), including internal e-mails, can cause quite a bit of damage. So if a company is required to communicate in a foreign language, make sure the day-to-day communicators have mastered the language sufficiently to prevent badly worded e-mails from being used against the company.
All employees should be informed about the possibility and conduct of discovery proceedings so that they realise that there are some things that should never be found in any e-mail or document. There is nothing new about this advice – but what is new is that e-mails can have a strange effect on some people, seducing them into believing that the normal common-sense rules no longer apply.

Educating employees in e-mail etiquette could prevent future headaches.

What measures can be taken?

The following measures may help a Dutch company to avoid or limit American e-discovery: If there is no need for products to be sold on the U.S. market, and not much can be gained there, it could be decided to explicitly exclude any resales on US territory. Furthermore, consideration could be given to special contractual clauses restricting discovery. Finally, strict rules could be introduced for e-mail traffic and the saving and deleting processes.

Can e-discovery be a good thing?

A Dutch company engaged in litigation is naturally concerned about shielding itself from the high cost of American style e-discovery, but in some circumstances e-discovery could serve as a litigation tool. Because US civil procedure allows discovery in the United States in Dutch legal proceedings, the sheer cost of the discovery process can be a useful means of forcing a settlement in pending Dutch litigation.

[1] Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, more commonly referred to as "the Hague Evidence Convention".

[2] *Wetboek van Burgerlijke Rechtsvordering* or "Rv".

[3] Unofficial translation. There are a few other articles in Dutch law that may be used to obtain information, but they do not really improve the discovery available under article 843a of the DCCP.

[4] Summary Proceedings Judge, Rotterdam Court, 25 June 2009, KG ZA 09 -1203 JOR 2009/250.

[5] Summary Proceedings Judge, Utrecht Court, 18 August 2010, LJN BN5864.

[6] The Hague Court, 30 December 2009, JOR 2010/41.

[7] See Attorney General Asser in his submission to the Dutch Supreme Court decision of 14 February 1992, NJ 1992, 245 (Note by P. van Schilfgaarde).

[8] Arts. 27-29, DCCP

E-DISCOVERY AND PRIVACY

Wolter Wefers Bettink

A Dutch company confronted with a discovery order issued by an American court faces a dilemma: how can it produce all the relevant documents while at the same time meeting its often conflicting obligations under the Dutch Data Protection Act[1] ("Act"), which implements in Dutch law the EU Data Protection Directive ("Directive").[2] Rule 26 of the US Federal Rules of Civil Procedure permits discovery of "any matter, not privileged, that is relevant to the claim or defence of any party…" While US Federal Courts have given the scope of discovery a broad interpretation, the Netherlands and many other EU member states have formed a more restrictive view. This is based on the fact that in most civil-law systems a party to litigation is less likely to be able to obtain the production of documents from the other parties. It is also based on restrictions imposed by the Directive.

The EU Data Protection Directive regulates the processing of personal data and its export from the EU.

4

The aim of the Directive is to protect the fundamental rights and freedoms of natural persons, in particular, the right to privacy with respect to the processing of personal data. As such, the Directive implements the European Convention on Human Rights and other international treaties.[3] In its study of cross-border discovery conflicts, the Sedona Conference (a research and education institute dedicated to the advancement of law) has provided a framework for the analysis of conflicts between discovery requirements and privacy law in the EU.[4] The study shows that US courts tend not to observe national law in the country where information is sought. Unless a respondent is truly threatened by criminal sanctions under a national blocking statute or data privacy laws, the US courts primarily applies a reasonableness standard to the evaluation of requests for production of documents from a foreign entity in the light of good faith efforts by the respondent.

Scope of EU privacy legislation

In deciding which information should be provided under a discovery request, American courts balance a number of factors, including whether compliance with the information request would undermine the interests of a foreign sovereign nation. Therefore, a good faith effort to meet a discovery request should take into account an analysis of what is allowed under EU and national data privacy legislation.

The first issue is the extent to which discovery is affected by such legislation. The answer is that almost any document, electronic or not, may fall under the privacy rules of the EU and its member states. In the Netherlands, the Directive and the Act apply to any processing of personal data by a data controller established in the Netherlands.

Personal data is broadly defined to include any data relating to an identified or identifiable natural person. This may be an employee or a business contact but also the addressee of correspondence. Therefore, e-mails – which form the bulk of the documents to be produced under a discovery order – are subject to the Act, since they contain the sender's and the receiver's names, which are personal data. And so, by association, are the data in that e-mail, even if it contains only information on business matters. Likewise, reports of meetings, internal memoranda and personal notes of meetings or telephone calls will be considered personal data if the names of attendants, addressees or conversation partners are identified therein. The Directive and the Act apply to the processing of personal data on the territory of a member state. Processing includes any operation in relation to the data, such as collection, recording, storage, retrieval, consultation, making available and transfer. Therefore, most if not all of the processing of documents to be performed in the course of discovery proceedings will be subject to the Act if performed by a data controller in the Netherlands.[5]

Sanctions

If a party in a US court case does not comply with pre-trial production requests of documents, the court may impose appropriate sanctions. It may dismiss the proceedings and render a default judgment if the failure to comply with a discovery order is due to wilfulness, bad faith or any other fault of the petitioner. The inability of the petitioner to comply does not justify dismissal.[6]

1

As a rule, US courts consider blocking statutes that prohibit or restrict the disclosure of documents on national territory for the purpose of complying with the orders of foreign authorities to be only a minor factor when making the proportionality analysis. This standpoint was based on lack of evidence that such blocking statutes are ever enforced.[7] However, in January 2008, a French lawyer was convicted of violating the French blocking statute. According to the Sedona Conference study, such a conviction may, in appropriate cases, be sufficient to tip the balance in favour of following the rules of the jurisdiction where data are being sought.[8] In fact, *In re Global Power Equipment Group Inc.*, the Court dismissed this argument. [9]

4

While blocking statutes have been looked upon unfavourably by US federal courts, the EU data protection regime has received a more considerate treatment. From the case of *In Re Vitamins Antitrust Litigation*,[10] it has been inferred that foreign legislation implementing the EU Data Protection Directive is at least entitled to be respected by US courts.[11] In *Salerno v. Lecia*

A 'blocking statute' forbid nationals of a country, in the interest of sovereignty and security, to cooperate with foreign discovery requests.

the court precluded the production of documents since this was not allowed under the EU Data Protection Directive and German legislation implementing that Directive. The relative deference given by US courts to EU data privacy legislation in comparison to blocking statutes apparently stems from the fact that this legislation is viewed as fulfilling a legitimate purpose, whereas blocking statutes are seen as having been enacted to provide defendants with an argument against disclosing documents.

Although the Directive was not enacted with discovery in mind, American commentators have pointed out, however, that it provides a means of circumventing US e-discovery production requests. This may make data privacy laws in the EU operate like a blocking statute.[12] Furthermore, in those cases where US courts have, in one form or another, accepted that the defendant cannot be forced to violate EU data protection rules, the defendant was found to have made all reasonable efforts to obey the disclosure order. Therefore, companies in the European Union that have received a discovery request should not merely rely on the protection granted by their national privacy legislation, but actively consider how to comply with the request without infringing the privacy legislation.

A simple choice?

The consequence of not obeying a discovery order issued by an American court may be to lose the case. On the other hand, the sanctions for a violation of the Act appear moderate,[13] so companies may choose to ignore the restrictions imposed by the Dutch legislation. However, the Dutch Data Protection Authority ("CBP")[14] may impose severe penalties to compel compliance with several statutory obligations (including the prohibitions against unauthorized international data transfers and the processing of sensitive data).

Violation of the Act may also carry other, more intangible penalties. If a company violates employees' privacy by shipping a mirror of the company's mail server or its internet logs to the US, without complying with the Act, this may lead to loud protests from the works council or union. In turn, this may trigger negative press coverage that may damage the company's reputation. This may cause the CBP to investigate the transfer of personal data to the United States. During that investigation, it may issue an order prohibiting future transfers, again subject to a penalty for non-compliance.

Meeting the statutory objectives

The Act contains several requirements for the processing of personal data that appear to restrict discovery operations in a manner that may not always be compatible with the broad scope of discovery orders issued by US courts. This may not necessarily be the case, however, since with the right preparation it is possible to meet most if not all of the requirements of the Act while at the same time complying with the American discovery request.

The discovery process involves different steps that require the processing of personal data. First, as soon as litigation is reasonably anticipated, the relevant documents must be retained and will have to be stored and kept available for as long as necessary for the litigation. This potentially conflicts with the requirements of EU privacy legislation that personal data may not be stored for a longer period than is necessary for achieving the purpose for which it was collected or subsequently processed. As a rule, such a purpose does not include litigation. Also, the data subjects involved will not have been informed beforehand that documents containing their personal data may be submitted in US litigation. However, if relevant documents turn out to have been destroyed at a time when the company was required to keep them available for litigation, this may result in the company losing the case in the US, even if destruction took place in accordance with that company's privacy policy. To avoid this, once litigation is reasonably anticipated, the company should immediately review its privacy policy and stop automatic deletion of copies of relevant documents.

Legitimate purpose

Under the Act, the processing of personal data is allowed if it is based on one of the grounds set out in article 8 (i.e. Article 7 of the Directive). One of these grounds is that the processing takes place with the data subject's consent. In the case of a discovery request, it may be worthwhile to try to obtain such consent if the data subjects involved are limited in number and can easily be reached. However, in most cases this will not be an option.

Another obstacle is that the consent must be freely given. It is questionable whether an employee can freely give consent after having been informed that this is necessary in connection with a discovery request received by his employer. Article 8 of the Act provides for two alternative routes. Under article 8(c), the processing of personal data is allowed if it is necessary for compliance with a legal obligation to which the controller is subject. Likewise, article 8(f) allows the processing necessary for the purposes of legitimate interests pursued by the controller or by the third party to whom the data are disclosed, except where such interests are overridden by the interest in ensuring the statutorily protected fundamental rights and freedoms of the data subject.

Although it may well be argued that complying with an American discovery request falls under the purpose of complying with a legal obligation pursuant to article 8(c), the Data Protection Working Party set up under Article 29 of the Directive – the advisory body on data protection for the European Commission – has stated that this purpose refers only to an obligation under the legislation of the member states, which would seem to exclude American legislation and US court orders.[15] Therefore, a safer route may be found in article 8(f) of the Act. According to the Data Protection Working Party, the selection of relevant documents in order to establish the facts in legal proceedings in the US may be a legitimate interest under this provision. Such an interest should in each case be balanced with the data subjects' fundamental right to privacy. This should

take into account the issues of proportionality, the relevance of the personal data to the litigation and the consequences for the data subject.[16] In addition, where sensitive data are concerned, such as health data, either the explicit consent of the data subject should be obtained or it should be argued that the processing is necessary for the establishment, exercise or defence of a legal claim (Article 8 of the Directive).

Proportionality

In executing the discovery request, other principles of the Act have to be observed as well. Thus, personal data must be processed fairly and lawfully and collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The processing must be adequate and not excessive in relation to the discovery order, accurate and, where necessary, kept up to date; and kept in a form which permits either identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

In particular, the requirement that the data not be processed for a purpose that is incompatible with the purpose for which they were collected may be difficult to align with a discovery request that requires that the receiving party has to produce "all relevant documents", including information that may lead to the discovery of relevant information. In this context, the Data Protection Working Party suggests that a first filtering stage should take place to determine which data are objectively relevant to the issues being litigated and to determine whether personal data are necessary or that the information could be reproduced in an anonymised or redacted form.

Although from a privacy standpoint the filtering activity should ideally be carried out locally in the EU member state where the personal data are located, the Data Protection Working Party recognises that it may be difficult to determine the appropriate person to decide on the relevance of the information, certainly within the strict time limits of the disclosure procedure. It suggests that this could be done by trusted third parties who are in the member state and who have a sufficient level of independence and trustworthiness (and knowledge of the litigation process) to do this. At present, such third parties are scarce in the EU and, therefore, it may not be realistic to require that the filtering be done locally. Therefore, it may be necessary to transfer all the data (in the form of a mirror of a hard drive and a copy of a server) to the United States where the selection of document is then carried out.

International transfer of personal data

For the transfer of personal data to a country "without an adequate level of protection" a permit is normally required from the Dutch Ministry of Justice. The permit application must be filed with the Dutch DPA, which advises the Minister on whether to grant of the permit. Like most countries outside the EEA, the US is not considered a country with an adequate level of protection. Under the

US Safe Harbour Regulation, a company that has adopted privacy policies that are equivalent to the EU's Data Protection Directive is considered to meet the requirements of that Directive. Transfer of personal data to those companies is allowed without a permit.[17] Since only a limited number of US companies are on this list, and since the personal data transferred in the course of discovery will also be shared with an American court and, if necessary, witnesses, juries, experts and opposing counsel, the Safe Harbour Regulation can in most cases of discovery not be used to avoid the permit requirement.

A permit will only be granted if an agreement is in place between the data controller and the receiving entity outside the EU. This agreement must conform to the standard contractual clauses of the European Commission (the "Model Clauses").[18] In addition, the CBP assesses in each individual case whether sufficient safeguards regarding data protection are in place. This assessment is particularly strict when sensitive data are involved. However, the Model Clauses do not restrict the further processing of personal data once they are in the US. The only condition is that the data and the third parties to whom they will be distributed are identified in the permit application.

As it usually takes three months or more to obtain a permit, this may be a hurdle to meeting a discovery order in time. However, by co-operating with the CBP from an early stage after receiving the discovery order this may be managed to some extent. We have found the CBP to be co-operative if all relevant information obtaining to the permit request is provided and the necessity for a speedy issuance of a permit is well explained.

Once a discovery request is received, the company should as soon as possible prepare a permit application and file this with the CBP.

Transparency

The Dutch Act also contains several provisions aimed at increasing transparency for data subjects. These may present practical hurdles in executing a discovery request. For instance, notice of each processing of personal data must be given to the CBP prior to the start of the activity. Notification is a fairly simple process, but care should be taken that it is completed before the processing of documents starts. The notification must specifically refer to the transfer of personal data to the United States in the context of discovery. It can be filed with the CBP by using a standard Dutch notification form and is effective immediately upon filing.

The Act requires that employees be informed of the processing and transfer of their personal data for the purpose of the discovery obligations prior to the start of the processing and transfer. At first, this may consist of a general notice informing employees of the possibility of data being processed, followed by a specific notice once the discovery request has been received. Such a

notice should specify the categories of data involved, the identity of persons to whom the data will be transferred and the purpose of the transfer. This can be done either by email, by placing a message on the intranet in an employee newsletter or by any other appropriate communication to employees. Employees and all other persons whose data are processed in the course of the discovery are entitled to request information on the processing of their personal data and may rectify, erase or block data if the processing does not comply with the provisions of the Act. The information should be provided by the data controller, which should also allow them access to the documents in case there is reason for rectification, erasure or blocking. The extent of this right of the data subject to control the processing of its personal data is still very much unclear.

In a recent case, a Dutch court held in the context of a personal injury claim that the claimant was entitled to a list of all documents containing personal data that the insurance company had in its possession and to copies of those documents not subject to privilege.[19] The latter restriction is in line with one of the basic principles of discovery that privileged documents are not to be disclosed. In the Netherlands, the concept of privilege is not as well developed as in the United States, so it is significant that the court recognized and respected the confidentiality of correspondence between lawyer and client.

Furthermore, the recent ruling by the European Court of Justice in Akzo v. European Commission[20] has clarified that in-house lawyer do not have the right to legal professional privilege in the context of EU anti-trust proceedings. Although this ruling is applicable to information discoverable in EU anti-trust proceedings it may be the beginning of a stricter view on what is privileged information in other proceedings as well, for example, under the Act. It is worth taking a close look at the digital investigation conducted by the Dutch Competition Authority described in a separate chapter in this guide.

Recommendations

A company should have a standard retention policy based on the data retention limits imposed by the Act.

Once a discovery request is received, the company should as soon as possible prepare a permit application and file this with the CBP. The company should liaise with the CBP in order to ensure that the permit is issued as soon as possible.

In addition, the employees involved should be informed which data will be processed, to whom they will be disclosed and for what purpose.

Privileged correspondence with its external lawyer does not need to be disclosed under either the discovery request or the Act, but memoranda and correspondence sent by its in-house lawyer may not be covered by privilege.

[1] Wet bescherming persoonsgegevens or "Wbp"

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Official Journal L 281, 23/11/1995 P. 0031 – 0050)

[3] Art. 12, Universal Declaration of Human Rights; Art. 17, UN International Covenant on Civil and Political Rights.

[4] "The Sedona Conference Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery", 2008.

[5] The Act also applies if the equipment used to process the data is (other than merely in transit) located in the Netherlands.

[6] Federal Rules of Civil Procedure 37(b)(2)(A)(v) and (vi). See also Societé Internationale pour Participation Industrielle et Commerciale, S.A. v. Rogers, 357 U.S. 197 (1958, p. 212).

[7] Bodner v. Paribas, 202 F.R.D. 370, 375 (2000) and the Strauss v. Crédit Lyonnais S.A., 242 F.R.D. 199 (E.D.N.V. May 25, 2007).

[8] Sedona Conference, p. 26. In that case litigants may be well advised to rely on the Hague Convention as a means of obtaining discovery abroad.

[9] 418 BR 833 - Bankr. Court, D. Delaware 2009.

[10] 2001 U.S. Dist LEXIS 8904 (D.D.C. June 20, 2001).

[11] Kristen Knapp, "Enforcement of U.S. Electronic Discovery Law against Foreign Companies: Should US Courts give effect to the EU Data Protection Directive?" Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm.

[12] Knapp 2008, ibid, warns US courts that they "should not succumb to the temptation of allowing companies to hide behind foreign data privacy statute as a means of escaping US jurisdiction for the purposes of e-discovery."

[13] Under the Act, a maximum fine of €4,500 can be imposed, but only for violating the duty to register data processing activities with the CBP.

[14] College bescherming persoonsgegevens or "CBP".

[15] Article 29 Data Protection Working Party, Working document 1/2009 on pre-trial discovery for cross-border civil litigation, 00339/09/EN (WP158).

[16] Ibid., page 10.

[17] For the list of the companies adhering to the Regulation see https://www.export.gov/safehrbr/list.aspx

[18] See http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm.

[19] Zutphen Court, 8 October 2009, 102240/HA RK 09-25, LJN BK 4206.

[20] Akzo v. European Commission, Court of Justice of the European Union, Case C-550/07, Decision of 14 September 2010.

SEIZURE OF ELECTRONIC DATA BY THE DUTCH COMPETITION AUTHORITY

Gerard van der Wal

The Dutch Competition Authority ("NMa")[1] is responsible for enforcing the Dutch Competition Act,[2] which prohibits cartel agreements and abuse of dominance in the market. In these electronic times, almost every investigation by the NMa includes a form of e-discovery. The NMa's policy rules with regard to the inspection of electronically stored materials have recently been amended to include a procedure for analogue and digital investigation.[3] It is worth taking a look at the NMa's digital investigation process, as it is not unlikely that other authorities monitoring legal compliance will adopt similar procedures in the future.

If the NMa decides to investigate a business ("undertaking") suspected of infringing competition law, the NMa's inspectors usually arrive at the undertaking's premises without formal notification or even informal warning. At the beginning of this unannounced investigation, the officials will provide a document stating the purpose and scope of the investigation (collectively referred here further as the "scope of the investigation"). The scope of the investigation may change as the investigation progresses. In that case, a new document stating the amended scope will be provided as soon as possible.

The electronic part of the investigation is conducted in three steps. First, the NMa identifies and selects potentially relevant information on the spot at the undertaking's premises. Second, in certain circumstances, a further selection of the information gathered may, at the undertaking's request, take place at the NMa's offices in The Hague. Third, the information finally selected is added to the "investigation data" that is the basis for carrying out the investigation. These three steps are discussed further below.

STEP 1: THE INVESTIGATION AT THE UNDERTAKING'S PREMISES

When searching for evidence of specified suspicious behaviour, the NMa classifies both analogue and electronic information or records (together referred to as "materials") into two categories:

materials within the scope of the investigation: materials that can reasonably fall within the scope of the investigation due to their nature and/or content; and

materials outside the scope of the investigation: materials that do not fall within the scope of the investigation, including private materials.

The investigator will collect all digital information that is considered to be within the scope of the investigation in a set of data identified as being "originally within the scope" (*origineel binnen de reikwijdte*). If at the undertaking's premises the investigator cannot rule out that a set of data also includes information outside the scope of the investigation, this set of data will be identified as being "possibly outside the scope" (*mogelijk buiten de reikwijdte*). In both cases, the undertaking investigated will receive a list of the electronic information.

Privileged information

Under the Dutch Competition Act, the NMa does not have the right to inspect information subject to legal professional privilege. In order to safeguard this privilege, the undertaking may indicate on the spot that certain material is privileged. If the NMa official agrees that this material is privileged (after, at most, a cursory look), the relevant information will not be included in the data sets if this is technically possible. However, should the official disagree, the NMa will take the material without examining it and hand it over to a special "legal privilege officer" (*functionaris verschoningsrecht*) at the NMa.

See the recent ruling by the European Court of Justice in *Akzo v. European Commission*, as described in the previous article, in which the court decided that information provided to and by in-house counsel is no longer considered privileged in EU anti-trust proceedings.

STEP 2: FILTERING AND FURTHER SELECTION AT THE NMA'S OFFICES

The NMa may filter the data sets at its offices in The Hague in order to discard any obviously irrelevant information. After this filtering, the NMa provides an overview of the electronic information in the remaining set of data. The NMa also provides a copy of the set of data to the relevant undertaking. Due to the differences in nature of the two types of data, the filtering procedure for data "originally within the scope" differs from the filtering procedure for the data "possibly outside the scope". This difference is based on the goal of preventing any unwanted information in the data set "possibly outside the scope" from being added to the "investigation data".

The procedure regarding the data "possibly outside the scope"

The general procedure is that the investigated undertaking has ten working days after the receipt of an overview and a copy of the set of data "possibly outside the scope" to indicate which information falls outside the scope of the investigation and why this is the case. The relevant official then verifies this claim, this verification being conducted in the presence of a representative of the undertaking involved. If the official agrees, the information is not added to the "investigation data". However, should the official disagree, the information is added to the "investigation data".

Privileged information

The undertaking being investigated has ten working days after the receipt of an overview and a copy of the data "originally within the scope" or the data "possibly outside the scope" to indicate which information is privileged. Furthermore, should the NMa have taken any information that was on the sport alleged to be privileged, the legal privilege officer will request the undertaking investigated to substantiate within ten working days its claim that certain materials are privileged.

In both situations, the legal privilege officer assesses the claim of privilege and decides whether it is justified. If the claim is justified, the undertaking concerned is informed accordingly. In that case, the relevant information is destroyed or returned to the undertaking. Should the legal privilege officer decide that the claim is unfounded, the undertaking concerned is given five working days to support its claim. Going through the process again, the legal privilege officer conducts an assessment of the claim in accordance with the procedure just described. Any relevant information found not to be privileged is added to the "investigation data" after five working days. This five-day period granted also provides the undertaking with time to apply to the court.

STEP 3: ADDITION TO THE "INVESTIGATION DATA"

In the final step, all the filtered data sets are added to the "investigation data". Once the investigation has been completed and the limitation periods for submitting an objection or appeal has expired, all relevant information is destroyed to the extent legally permitted, except for the information on which the NMa's decision is based. At the same time, all information exchanged between the undertaking and the legal privilege officer will be destroyed to the extent legally permitted.

[1] Nederlandse Mededingingsautoriteit or "NMa".

[2] Mededingingswet or "Mw".

[3] "Werkwijze NMa analoog en digitaal rechercheren", Netherlands Government Gazette [Staatscourant]16 August 2010, no. 12871.

E-DISCOVERY IN INTERNATIONAL ARBITRATION

Dirk Knottenbelt

There is not much in the literature about current practices in international arbitration regarding the discovery of electronically stored information.[1] Despite efforts to keep limited discovery one of the hallmarks of arbitration and this being one of its primary cost-containment features, it is clear that the trend is for parties to demand, and for arbitrators to permit, more expansive discovery.

The generation and production of e-mails and e-mailed information, in particular, has led to an "e-discovery revolution" that has posed new challenges in its complexity and dimension.

Discovery in international arbitration

In international arbitration, discovery is considerably more limited than in court proceedings, especially US court proceedings. The rules of civil procedure do not apply to arbitration unless the parties provide for this in their arbitration agreement. Typically, the scope of discovery is determined by the agreement of the parties when entering into the arbitration agreement or during the arbitration itself. The scope of discovery is also determined by the arbitral tribunal on the basis of the submissions of the parties and the interpretation of the applicable arbitration rules.

The discovery-related expectations of the various parties and arbitrators may be quite different. This is particularly true in arbitrations in which the parties come from both civil-law and common-law jurisdictions. Generally, in civil-law jurisdictions, the parties are relatively immune from orders to produce documents. Disputes are decided on the basis of the documents voluntarily submitted by the parties. As such, lawyers and arbitrators based in civil-law countries tend to dislike American discovery practices in particular, which they perceive as being potentially abusive and excessively expensive. Consequently, they are not easily swayed by arguments that discovery, even less extensive discovery, is vital or indispensable to proper adjudication in international arbitration.

Indeed, even lawyers and arbitrators from other common-law jurisdictions (e.g. in the United Kingdom or Canada) often distance themselves from American-style discovery.

Another fundamental difference between discovery in American litigation and in international arbitration is the allocation of costs. In American litigation, each party traditionally bears its own costs. In international arbitration, however, an arbitral tribunal generally makes a discretionary determination of how the arbitration costs are to be allocated. The tribunal could allow the unsuccessful party to pay the costs of the arbitration in whole or in part, including the discovery costs.

This may explain in part why in international arbitration the scope of discovery, and not its cost allocation, tends to be more of an issue.

For these reasons, American and non-American parties and arbitrators come to international arbitration with different assumptions and expectations. American parties may expect that more discovery will be allowed. Accordingly, they may have diligently preserved more documents, even those detrimental to their case. On the other hand, parties from other jurisdictions may not expect at all to be required to share adverse documents with the other party or the arbitral tribunal. Typically, such parties only produce documents they believe will support their claims or defences. Requests for documents submitted to them must be supported by a showing of need, together with a narrow description of the documents and the statement that the document actually is in the possession of the other party. In rulings made by arbitrators on the scope of compulsory document production, non-American parties generally expect arbitrators to balance the likely benefits of production against the cost, delay and burden borne by the party who must produce it.

E-discovery in international arbitration

The question is whether the law or the existing arbitration rules offer any guidance in determining the standards for e-discovery in international arbitration. If the seat of the arbitration is in the Netherlands, Dutch civil procedure is the law applicable to the arbitration proceedings (*lex arbitri*).

Dutch civil procedure offers little guidance on the scope of discovery in arbitration. Article 1039(4) of the Dutch Code of Civil Proceedings ("DCCP") allows an arbitrator to order the production of documents. Although no further guidance is offered, it is generally accepted that the requesting party must show that it has an interest in the production of the documents and must specify which documents it is seeking.

Generally, the *lex arbitri* provides broad and non-specific rules that will say, e.g., that the parties must be treated with equality; however, the rules do not go into detail about how this is to be achieved in terms of the exchange of pleadings, witness statements, documents, and so forth.

In arbitral proceedings parties as well as the arbitrators may not have the same understanding of e-discovery, especially where the parties come from civil and common law jurisdictions.

In arbitration, the parties are generally free to determine and specify the procedural rules that govern their arbitral proceedings, including the type and scope of discovery permitted. Yet parties to a commercial agreement are often unwilling to seriously contemplate, let alone negotiate, detailed discovery procedures that would apply in the event a dispute arises. Furthermore, contractual parties frequently cannot predict their discovery needs until the dispute materialises, making prior consideration of arbitral discovery even more difficult.

In practice, therefore, contractual parties rarely detail the arbitration procedure to be followed, instead designating the rules of one of the major international arbitration institutes (e.g. ICC, ICSID, ICDR or LCIA) as applicable. If the parties prefer not to use an institute to administer the arbitration, the UNCITRAL Arbitration Rules are frequently chosen.

All of these rules provide that the arbitrators may, at the request of one of the parties, order another party to produce certain documents.[2] None of these rules, however, provide any real guidance on the scope of appropriate discovery. It is often up to the tribunal to determine the scope, the only guidance being the general rule to accord the parties due process, i.e. the right to be heard and a fair opportunity to present its case.

8

IBA Rules on Taking Evidence

To fill the perceived lack of guidance for discovery in institutional international arbitration, in 1999 the IBA prepared the IBA Rules on Taking Evidence ("IBA Rules").[3] The IBA Rules explicitly contemplate that there will be prehearing discovery, albeit within a scope considerably narrower than provided for in American litigation. The drafters considered "expansive American or English-style discovery" to be inappropriate in international arbitration. Their primary concern was not to open the door for "fishing expeditions". Accordingly, the IBA Rules require requests for document production to be carefully tailored to issues that are relevant to the determination of the merits of the case.

The IBA Rules do not specifically deal with e-discovery.[4] Nevertheless, the following principles embodied in the IBA Rules could help the parties and arbitrators to resolve e-discovery disputes, especially those involving the scope of e-discovery.

- Specificity - The IBA Rules require a specific description of the document sufficient to identify it, or a narrow and specific description of a particular category of documents.

- Materiality - The IBA Rules require a description of how the requested documents are "material to the outcome of the case".

- Unavailability to requesting party - The IBA Rules require that the requested documents be "not in the possession, custody or control of the requesting party".

- Availability to other party - The IBA Rules require the requesting party to explain why it believes the requested information is in the possession of the other party.

- Not a relative financial burden - The IBA Rules provide that fairness ("considerations of fairness or equality of the parties") is another factor that the tribunal should use to determine whether a discovery request should be granted.

- Not an unreasonable burden - The IBA Rules provide that a discovery request should not be granted if production places an "unreasonable burden" on the responding party.

All of the above principles are useful for arbitrators in determining the scope of e-discovery, the proportionality and the cost allocation, i.e. who should pay for the discovery. On that basis, applying the IBA Rules to institutional or ad hoc arbitration could provide the parties and the arbitrators real guidance on the scope of appropriate discovery.

Protocol for e-disclosure in arbitration

However helpful the IBA Rules may be, however, the above principles remain open for interpretation An arbitrator from a common-law country will apply a different interpretation than a civil-law arbitrator. The IBA Rules, therefore, only offer guidance within the legal framework in which the arbitration is conducted.

This has resulted in various protocols that guide parties and arbitrators in the conduct of e-discovery. As such, the parties may chose to apply, for instance, the Protocol for e-Disclosure in Arbitration of the Chartered Institute of Arbitrators.[5]

The Protocol is intended to achieve early consideration of e-discovery for the avoidance of unnecessary costs and delay and to focus the parties and the tribunal on the scope and conduct of e-discovery.

Arbitration agreement

Contractual parties may wish to consider including e-disclosure-related provisions in the arbitration clause in contracts in the following circumstances: the potentially disclosable documents are in electronic form, the time and costs for allowing discovery may be an issue, or the scope of e-discovery may lead to a dispute between the parties (e.g. the different backgrounds and, hence, the different expectations

In contracts with a US party it is normally not possible to agree on an exclusion or limitation of discovery. In such case, one may seek to contain the scope and consequences of e-discovery.

of the parties). Although it is possible to expressly exclude or limit the possibilities of discovery in an arbitration agreement, even if a contract is subject to US law and the place of arbitration is in the US, in contracts with a US party it is normally not possible to agree on such exclusion or limitation. In this case, one may seek to contain the scope and consequences of e-discovery in a more detailed, made-to-measure arbitration clause.

Such provisions should define what constitutes the voluntary "first tier of discovery" of electronic documents in the earliest stages of the arbitration proceedings. This will allow the parties to expedite the process by defining the following:

- the scope of any e-discovery,
- the format in which electronically stored information in support of a claim or defence will be provided,
- the time period during which discovery exchanges will occur,
- the possible search technologies that are to be applied,
- the nature and characteristics of each party's data storage system,
- the allocation of costs incurred in producing electronically stored information, and
- the inadvertent disclosure of privileged documents and the preservation of electronically stored evidence.

The management of any subsequent stages of discovery can also be addressed and facilitated.

Including provisions in the arbitration agreement that direct the parties to make voluntary and early exchanges of electronically stored information and that specify the content and timing of such exchanges is in accordance with the Sedona Principles[6] and better serves the values that have historically characterized arbitration as a less costly, more efficient and speedier forum for alternative dispute resolution.

[1] Electronically stored information, for the purpose of the US Federal Rules of Civil Procedure (FRCP) is information created, manipulated, communicated, stored, and best utilized in digital form, requiring the use of computer hardware and software. The term has become a legally defined phrase as the U.S. government determined for the purposes of the FRCP rules of 2006 that promulgating procedures for maintenance and discovery for electronically stored information was necessary.

[2] Article 20(5), ICC Rules (www.iccwbo.org/uploadedFiles/Court/Arbitration/other/rules_arb_english.pdf);
Article 34(2), ICSID Rules (http://icsid.worldbank.org/ICSID/ICSID/RulesMain.jsp);
Article 19(3), ICDR Rules (www.adr.org/sp.asp?id=33994);
Article 22.1(e), LCIA Rules (www.lcia.org/Dispute_Resolution_Services/LCIA_Arbitration_Rules.aspx#article22).

[3] Latest version of 29 May 2010 (www.ibanet.org/Publications/publications_IBA_guides_and_free_materials.aspx).

[4] The ICC has, meanwhile, constituted task forces to study and identify the essential features and effects of e-discovery in international arbitration.

[5] For the text, see <http://www.ciarb.org/information-and-resources/E-Discolusure%20in%20Arbitration.pdf>.

[6] The Sedona Principles are a set of 14 principles that were developed by members of the Sedona Conference in the US in order to provide a common approach for managing the discovery process as it changes with technology. These widely cited rules are designed specifically to bring order to the chaos that has characterized electronic discovery. (<http://www.thesedonaconference.org/content/miscFiles/TSC_PRINCP_2nd_ed_607.pdf>).

DISCOVERY AND DISCLOSURE IN THE 21ST CENTURY

John Payton

Origin of discovery and disclosure

E-discovery is just the latest permutation of an age old practice in common-law litigation called "discovery" (in the US) and "disclosure" (in the UK and other common-law jurisdictions). Introduced into English law as early as the 1840s, this practice was intended to enhance judicial efficiency and, especially, the fairness of the legal process. This was a time in the development of English law during which the fairness of the justice system had come under increased scrutiny – unsurprising in an era in which a man could be convicted of theft after a trial of only 2 minutes and 53 seconds and a judge's instruction to the jury of only ten words: "Gentlemen, I suppose you have no doubt? I have none"[1].

Partly in reaction to such abuses, it came to be considered unfair to deprive a litigant of relevant, even dispositive, evidence merely because it was in the hands of the other party. It was also thought that if the parties both knew more about the strengths and weaknesses of each other's position, they would be more likely to settle obvious cases without going all the way to trial, thereby saving the court's time and allowing judges to focus on the really difficult cases. In 2010, the day-to-day reality concerning discovery disputes often significantly erodes the judicial efficiency hoped for. Still, overall fairness continues to be a valid aspect of discovery.

Governing rules

Discovery, including e-discovery, is governed by the applicable procedural rules of the court, arbitral tribunal or other dispute resolution mechanism before which a given matter is being adjudicated (hereinafter, I will refer to all of these as "litigation"). In the United States, most litigation that a Dutch company is likely to be involved in will be heard in one of the federal district courts. Rule 26 of the Federal Rules of Civil Procedure governs discovery before these federal district courts.[2] Keep in mind that each of these courts may also have specific supplemental local rules. It is also possible – although unlikely – for a Dutch company to be involved in issues governed solely by the laws of one of the US states or territories. In this case, discovery would be governed by that state's procedural rules, including the local variations.

In England and Wales, the practice of disclosure is strongly influenced by the practice directives of the Law Society.

General tips

Regardless of the situation you find yourself in, it is always important to follow the instructions of local counsel who are familiar with the local rules and procedures. This is certainly the case when it comes to US court proceedings. At the same time, it will be beneficial to constantly challenge your lawyer's instructions, not necessarily to save yourself some e-discovery effort, but primarily to make sure you understand exactly what you are being asked to do and why.

Understanding what your US attorney is asking of you will help him win your case.

Discovery is often handled most directly by the youngest and most junior associates. Their careers and jobs depend on not making mistakes and not missing a thing. Therefore, they are likely to demand a much more thorough and pervasive search for e-documents than your case may require. Moreover, their understanding of the various IT applications in your company may be as limited as their experience as lawyers.

They are also not usually the most experienced lawyers when it comes to communicating complex and uniquely American legal concepts and jargon to people whose first language is not English. Don't let your pride in your own English language ability seduce you into making the mistake of assuming you know what they "must surely mean." Keep asking them questions until you are sure you fully understand what they actually do mean.

Legal hold

As the officers of Enron and Arthur Andersen learned to their great regret, US law requires parties – starting from the moment when litigation may be reasonably anticipated – to preserve and not destroy any document relevant to litigation. This is referred to as the "legal hold". The first thing your US lawyer will ask you to do is to make a list of each employee who participated in any meaningful way in the event or activity that gave rise to the litigation. These employees are referred to as "custodians" as they will have created, received and/or had direct access to documents which form potentially relevant evidence. They are the "custodians" of the evidence.

Each custodian identified will be given a "legal-hold notice", drafted by your lawyers, instructing them to preserve and not destroy any document potentially relevant to the litigation. Many vendors offer legal-hold management software. Modern IT systems enable the automatic preservation of

most electronic information, making it difficult or impossible for employees to delete, whether intentionally or accidently, any relevant information. Identifying and evaluating the business case for acquiring such software is a task that requires the cooperation and involvement of the IT department, the legal department and the business managers.

I ELEMENTS OF DISCOVERY

Timing and content

The three major elements of discovery are "depositions" (*getuigengehoor*), "interrogatories" (written questions to the opposing party) and "document requests" (which includes e-discovery). Typically, litigation begins with the plaintiff filing a "complaint", followed by the defendant's "answer". Some preliminary motions overlapping the discovery phase may have to be dealt with. Discovery usually begins within a few months after the initial complaint has been filed and can continue for months and even years, although at some point the judge will set a deadline for the production of the requested information, documents and things.

Interrogatories

The interrogatories always request the opposing party to identify its employees who have had some connection with the events or activities that have given rise to the litigation. They will also ask for admissions and explanations of the circumstances surrounding these events or activities and the addresses and organization charts of the entities or departments involved. They may also seek explanations of how the company is organized and managed, including chains of command and formal and informal reporting lines. The plaintiff usually begins the discovery phase by serving its interrogatories and its document request. The defendant follows with the defendant's own requests.

Document requests

Document requests generally ask the opposing party to send the requesting party each and every bit of information that is in any way related to the events or activities that gave rise to the litigation. They may also ask for physical objects (e.g. an example of a defective product), copies of any of the following provided they are relevant to the subject matter of the litigation:

- company policies,
- web sites,
- e-mail,
- text messages,
- Blackberry content,
- schedules,
- Power Point presentations,
- Excel sheets,

Any information recorded in any way is subject to discovery.

- databases,
- SAP and other accounting program records,
- recorded voice mails,
- recorded "chat" files,
- training and marketing videos,
- transcripts or recordings of video or audio conference calls,
- notes of meetings,
- handwritten comments in the margins of any other documents,
- etc., etc., etc., etc., *ad nausea*.

Any information recorded in any way is subject to discovery. Through the 1990s, most document discovery was paper-based. This has so dramatically changed in the last five years that paper files have become almost a novelty (but must not be forgotten). During the 1990s, it was unusual for the evidence in litigation to reach a million pages. Today, the average business user adds a gigabyte (100,000 pages) of data to his or her e-mail account each year. If ten people are involved and the litigation covers a five-year period, that's five million pages for a relatively small case. More complex litigation can run to terabytes and e-discovery vendors speak in terms of "peta-bytes" for major government litigation. The defendant may object to document requests within 30 to 60 days. Eventually, the judge will decide what must be produced. Objections may be based on the following.

You may not refuse to disclose any information solely because it is "secret" or "sensitive" or "confidential."

- The request is too broadly phrased. Defendants often state that they will produce relevant documents within a narrower, self-defined scope.
- The requested information is not relevant to the matter being litigated.
- The request is not reasonably expected to lead to the discovery of admissible evidence.
- The request places an unreasonable burden on the responding party in relation to the potential value to the requesting party.

But a defendant may not refuse to disclose information solely because it is "secret" or "sensitive" or "confidential." These issues can, to a limited degree, be covered by a "protective order" negotiated between the parties and issued by the judge.

Depositions

Depositions are interviews of your employees conducted by the lawyers of the other party. Your own lawyers will also be present to protect your rights, but there is no judge or jury present. Depositions are generally video-taped and excerpts of the depositions may be introduced in court as evidence. A typical deposition will last less than one day, but can go on for a week or more depending on the subject matter and the involvement of the deponent. Documents and information collected by the deposing party during the earlier stages of discovery may be used to draw out damaging evidence and admissions from the deponent. Preparing a deponent usually requires four to eight hours. The lawyer will train the deponent to answer only the question asked and to avoid helping the other party to understand.

II PREPARING FOR E-DISCOVERY

Document retention

The best preparation for discovery is having a good policy on document retention and records management policy and ensuring that this policy is properly and consistently applied, enforced and periodically updated. The goal of any such policy should be to create documents appropriately, securely retain the information having business or legal value, destroy information that does not have, or that loses, its business or legal value, and comply with applicable legal holds.

A well organized filing and archiving system will pay dividends when e-discovery is upon you.

11

Part of the implementation of such policies should include establishing a coherent filing structure so that the information retained can be located quickly when needed, not for e-discovery purposes, but for business purposes. It is generally too expensive to maintain a document retention regime designed solely as a precaution against that unhoped-for day when a complaint lands in your in-box. You should organize your documents in accordance with your business needs; however, a well-organized filing and archiving system will pay dividends if e-discovery is ever thrust upon you.

Role of the legal department

The legal department at a large organization bears the brunt of responding to common-law litigation and has the responsibility of preparing the company to respond quickly and effectively. US-based plaintiffs wishing to sue Dutch companies may use the procedure established by the Hague Service Convention.[3]

Many non-US companies with subsidiaries in the US may find that plaintiffs try to serve complaints on the Dutch parent by serving the US subsidiary. While such service may not be formally effective

under the applicable rules of civil procedure, judges will frequently consider that the Dutch parent did, for all practical purposes, have constructive notice of the lawsuit. If so, the relevant time periods will start to run. Most especially, the obligation to preserve potentially relevant documents will be in effect. The legal department must be sure that there are procedures in place so that mailroom personnel and building receptionists recognize attempts at service of complaints and inform the legal department and upper management immediately. The goal is to ensure that deadlines do not pass without the company even being aware it has been sued.

6

Role of the IT department

The IT department will play an increasingly important role in the identification and collection of electronically stored information. At an early stage in the discovery process, Rule 26(f) of the Federal Rules of Civil Procedure requires the lawyers of the parties to "meet and confer" to exchange information about each party's electronic storage media and business software in an effort to reach agreement as to what sources of electronically stored information are reasonable to search for relevant documents.

It is essential for your lawyers to understand the IT systems of your company. It is worthwhile to have IT prepare a data map of all software programs (Microsoft Office, SAP etc.), e-mail, servers, back-up facilities and other aspects of your company's electronic document creation and storage infrastructure and systems. The IT and legal departments need to cooperate on a continuing basis, not only during contract negotiations for new software and IT services, but also in the selection of services that will be e-discovery-friendly in the future.

11

Role of the human resources department

For many companies without a strong central filing system and/or with poor archiving habits (i.e. most companies), the primary point of access to documents relevant to litigation will be the employees who participated in the events or activities that gave rise to the litigation. The human resources department (HRM) is ideally suited to help your lawyers understand the responsibilities on each custodian throughout the entire period relevant to the litigation. A good working relationship between the legal and human resources departments will help you collect this information quickly, thereby giving your lawyers a quick insight into your structure and the way your company does its business.

III ACTIVE E-DISCOVERY

First steps

The early stages of litigation consist of the preliminary mandatory pleadings and the delaying tactics that occur as a result of preliminary and interlocutory motions. This can take up months or even years. Thereafter comes the stage of litigation in which e-discovery must be begun in

earnest. Rule 26(a)(1)[4] of the Federal Rules of Civil Procedure requires that certain essential and non-controversial information be provided without waiting for a document request, including the names of custodians, a description and the location of the evidence the disclosing party intends to rely upon and a calculation of the damages claimed with supporting documentation. In practice, the company provides everything to its own outside lawyer, who then determines exactly what needs to be passed on to the other party. Even while the parties continue to argue about the scope of e-discovery, preservation of documents (including legal hold notices) and the collection of the most relevant potential evidence will be carried out.

Discovery team

e-Discovery requires a great deal of effort and the attention of various disciplines. An in-house legal counsel familiar with the business activity most intimately involved in the litigation should head up the discovery team. This lead in-house legal counsel will be the primary contact point with the external lawyers and an intermediary between them and management. This counsel will be responsible for advising management about the progress of the litigation and the settlement dynamics. In large cases, a second in-house legal counsel will take the lead in e-discovery matters. This counsel will coordinate with IT, HRM, the custodians and the outside lawyers with respect to the actual identification and collection of the potential evidence. At the very active stages of e-discovery, these responsibilities will be more than a full-time job and other work will need to be taken over by colleagues. At least one central IT specialist should be in the team to assist in instructing local IT engineers and/or IT service vendors in making defensible, encrypted copies of e-mail files and other electronic documents and coordinating the registration and shipping of the copies to the attorneys or the vendor of the document hosting and review platform. Depending on the complexity of the company's structure, it may be sensible to have a representative and contact within HRM.

Early case assessment

The sooner you know the extent of any wrongdoing or mistakes by your own employees, the earlier you can assess the potential damages you may be liable for. Knowing the whole truth about your real position can be of great benefit when deciding whether or not to settle and for what amount. The more information you have and the earlier you have it, the better you are able to assess the true risks. Keep in mind that even modest cases will cost at least €10,000 to €50,000 a month in legal fees. Major litigation costs can run into the millions each year. The earlier you can reach a reasonable settlement, the earlier you can stop the bleeding. Accurate knowledge of your true position is the key to reaching a reasonable settlement.

Preliminary interviews and document collection

The primary tool for early case assessment is the early interview of those most directly involved in the event or activity that gave rise to the litigation. These interviews are usually conducted jointly

by outside lawyers and in-house legal counsel with the outside lawyer taking the lead. Relevant documents are collected on an *ad hoc* basis, usually by dragging and dropping files to a USB stick. Documents collected at this stage are especially useful for gaining an insight into the litigation. However, the metadata of electronic documents is almost always corrupted during such informal collection and the evidentiary value of such documents can be degraded. The exact same documents collected systematically according to a consistent and reproducible IT process are usually required by the court.

Document collection interviews

All custodians need to be interviewed in order to determine what part they may have played in the subject matter of the litigation and what documents they have that may be relevant. These interviews often lead to the discovery of additional custodians, who will need to receive a legal hold notice and be interviewed. Other interviews of a more substantive nature will follow as your lawyers get more familiar with the case.

Document collection

The most important thing about document collection itself is to document and register what it is you have collected. It is best to use a database to keep track of both the custodians and the document collection, but a list on an Excel sheet is the most commonly used method. The list should contain the name, location, e-mail address, function and telephone number of each custodian as well as each kind of data that has been collected and the date of collection. Types of data include paper files (properly registered, a dying black art), current e-mail account, e-mail from any previous e-mail system, private e-mail account if ever used for business purposes, e-mail archives, and information stored on portable hard drives, CD, DVD, USB sticks, network drives, shared drives, computer hard drive, remote file server etc.

Copies of electronic documents must be made in a way that preserves the original metadata associated with such files. Back-up tapes have not traditionally been the subject of e-discovery unless there was evidence that a party had significantly failed in its duty to preserve documents pursuant to the legal hold. The cost of restoring the tapes to a live system for read-out was considered unreasonable. However, as more back-up services move to server-based back-up technology, these costs become more reasonable and I expect to see more cases in which back-up caches are required to be produced.

Copying electronic files

Most judges and US lawyers prefer forensic bit-to-bit images of the hard drives of custodians. This process is almost always done by a third-party vendor. It requires the custodian to give up his or her computer for about an hour. The hard drive is removed and copied onto a machine that copies every bit, including the deleted files to the extent they have not been overwritten.

Forensic software tools can then recover deleted files, if necessary. There are software tools available which promise users that they can erase deleted files without a trace. These promises are not true. Some employees are tempted to use such software to delete "private" information from their computers prior to imaging. Such deletions always show up and often lead to termination of employment or other sever sanctions – think of the Enron executives now enjoying prison hospitality.

A less intrusive way of copying is to use the "RoboCopy" tool provided by Microsoft with its Help Desk and Administrator software packages. This software can be used to copy the hard drives through the network while the user continues to use the computer. It does not copy deleted files, but preserves the original metadata, thus satisfying the authenticity demands of most US courts. Copies can be made to any number of media, but portable hard drives and USB sticks are growing in popularity over CD and DVD. The media should be encrypted before being sent to the US lawyer or data hosting and review platform vendor.

Hosting and review platform

All this information being collected is usually sent to an "e-discovery vendor". Paper files are scanned and converted to searchable pdf or tiff files. These files are then processed with optical character-recognition software to make them searchable. This vendor first converts all the various file formats (pdf, tiff, doc, excel, ppt – there are up to 400 of these) into a single format such as xml. In this way all of the data can be indexed and made searchable in one pass rather requiring multiple applications of the same search criteria to different types of files. Duplicate and non-relevant file types (e.g. .exe) are removed. The remaining data is loaded on a dedicated server with powerful search engine software, the review platform. Most vendors have their own proprietary search technology.

Selecting the proper vendor is usually left to the lawyers, who usually select the vendor they are most familiar with. This has the advantage of making the review of documents by the lawyers more efficient. This is important because the largest cost element of this entire process is the hours of lawyer time used in the searching. However, your company will pay all the costs of initial processing, hosting the data (price per gigabyte per month) and the technical assistance rendered to the lawyers. Each vendor has its own pricing model; they are all very different. If your company has a consistently high load of this kind of work, you may consider making the use of a single vendor standard and negotiating a quantity discount. Using the same vendor also gives you the option of training up your in-house lawyers to use the powerful search tools of the vendor for smaller scale investigations and early case assessment.

Production

Once the lawyers have had a chance to search and examine the search results, the documents your lawyers decide are relevant must be sent to the lawyers of the other party. Privileged documents

(usually communications between lawyers and their clients either requesting or consisting of legal advice) do not need to be produced. Production is done in accordance with a written agreement between the parties. Documents are usually produced electronically, together with their original metadata in original format. Each page is given a unique "Bates" number (this being the name of the manufacturer of the numbering machine formerly used to apply the numbers).

The distribution of documents produced can be limited by means of a protective order negotiated between the parties and approved by the judge. Even under a protective order, most documents can be shared by the lawyers with their client. Documents with significant current business value and sensitivity (designated as "confidential") are restricted to viewing by the lawyers and selected agreed-to employees who agree not to share the information with others in the opposing company. More sensitive documents (designated as "highly confidential"), may only be viewed by the lawyers. This protection can be undone if the other side's lawyers introduce a confidential or highly confidential document in court as evidence.

In exceptional circumstances, a judge may be persuaded to continue the protection by requiring that the evidence be submitted "under seal." This kind of continued protection is usually applied only to information the disclosure of which might create a danger to the public, information related to a patentable invention not yet applied for and other very specific and limited situations .

Additional reading

The Sedona Conference[5] is a think tank and legal education institute that has produced the leading publications on the topic of e-discovery. You can download their publications free of charge from their website. Another useful tool for understanding the e-discovery process is the Electronic Discovery Reference Model (EDRM)[6]. Most vendors use this model to assist you in evaluating their products and services.

Conclusion

I have given you more insight into the US litigation process in general and the e-discovery aspects of document collection and management in particular. There are too many variations for this article to cover this ground comprehensively. I do hope this article will give you a basis for challenging the advice of your lawyers, but in the end make sure you understand what they are advising and please do follow their advice.

[1] As quoted in R v. H (Appellant) (2003) (On Appeal from the Court of Appeal (Criminal Division)) R v. C (Appellant) (On Appeal from the Court of Appeal (Criminal Division)) (Conjoined Appeals), see the following link at item 11: http://www.publications.parliament.uk/pa/ld200304/ldjudgmt/jd040205/hc-1.htm

[2] http://www.ilnd.uscourts.gov/LEGAL/frcpweb/frc00029.htm

[3] http://www.hagueservice.net/hsc.html

[4] http://www.ilnd.uscourts.gov/LEGAL/frcpweb/frc00029.htm

[5] http://www.thesedonaconference.org/

[6] http://edrm.net/

PROFILES

Gary DiBianco is a partner in the London office of Skadden, Arps, Slate, Meagher & Flom, LLP, where he heads the London-based Corporate Investigations practice.
T: 44 20 7519 7258
gary.dibianco@skadden.com

John Payton is a US attorney at law operating in the Netherlands and advises large corporations on e-discovery.
T: 31 6 2249 6023
john@payton.nl

Marielle Koppenol-Laforce is a partner with Houthoff Buruma advising on conflict-of-laws and representing clients in international litigation and arbitration.
T: 31 10 21 72 525
m.koppenol@houthoff.com

Wolter Wefers Bettink is a partner with Houthoff Buruma specialising in IP, IT, e-business and privacy law.
T: 31 20 60 56 167
w.bettink@houthoff.com

Dirk Knottenbelt is a partner with Houthoff Buruma representing clients in international arbitration as well as being an arbitrator.
T: 31 10 21 72 472
d.knottenbelt@houthoff.com

Gerard van der Wal is a partner with Houthoff Buruma who's practice covers both national and European competition law.
T: 32 25 07 98 11
g.van.der.wal@houthoff.com

HOUTHOFF BURUMA OFFICES

Amsterdam
Houthoff Buruma
Postbus 75505
1070 AM Amsterdam
Gustav Mahlerplein 50
1082 MA Amsterdam
Nederland
T +31 (0)20 605 60 00

Den Haag
Houthoff Buruma
Postbus 305
2501 CH Den Haag
Noordeinde 33
2514 GC Den Haag
Nederland
T +31 (0)70 302 35 00

Rotterdam
Houthoff Buruma
Postbus 1507
3000 BM Rotterdam
Weena 355
3013 AL Rotterdam
Nederland
T +31 (0)10 217 20 00

Brussel
Houthoff Buruma België B.V.
Keizerslaan 5
1000 Brussel
België
T +32 (0)2 507 98 00

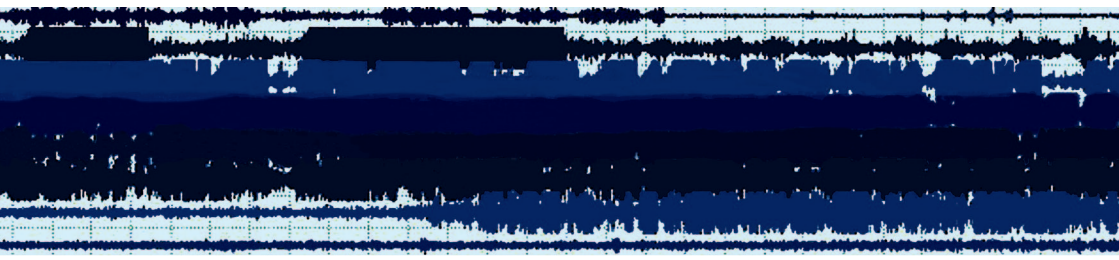
London
Houthoff Buruma Londen B.V.
33 Sun Street
London EC2M 2PY
United Kingdom
T +44 (0)20 7422 5050

www.houthoff.com

Content co-ordination: Lisa Hakanson (Houthoff Buruma)
Editing: Greg Korbee (Houthoff Buruma)

THE LAWYER
www.thelawyer.com
EUROPEAN AWARDS 2010
WINNER
Law Firm of the Year: Benelux

For more information on Houthoff Buruma see www.houthoff.com.



WWW.HOUTHOFF.COM