



Articles

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

Cross Border E-Discovery

How to manage potential evidence in an international environment

In the context of internal or regulatory investigations or other legal proceedings, companies located in Europe may be forced to disclose electronically stored information such as e-mails on short notice in order to comply with any such internal or regulatory request or applicable procedural electronic discovery regulations. These disclosure requirements may have considerable breadth, and non-compliance can lead to severe sanctions.

*Part I of this article describes the American procedure of e-discovery. Part II provides a brief description of the British concept of e-disclosure and considers how it differs from the American concepts of e-discovery. Part III shows – as one prominent example for civil code jurisdictions in the European Union (for an overview of other jurisdictions see *The Sedona Conference, International Overview of Discovery, Data Privacy and Disclosure Requirements*, September 2009) – the German regime for e-discovery requests and highlights some data protection issues to be observed. Part IV examines how the conflict existing between the common law concept of e-evidence and the civil law principles could be harmonized. Finally, part V gives some examples of how technology can be used to support e-discovery and to establish processes in compliance with applicable data privacy laws.*

I. The American Procedure of E-Discovery

Unlike in many civil law countries, the process of “pre-trial-discovery” is an important, costly, and timely part of the American legal system. It is at this pre-trial discovery stage that issues relating to e-discovery arise. The purpose of this judicial preliminary process is the finding of facts and/or discovery of the relevant evidence and is, to a large extent, conducted by the parties without the participation of judges. During this process, the parties can demand from their adversaries the presentation of comprehensive information concerning all facts and evidence which could be “relevant” to the alleged claim or defense, according to Rule 26 of the Federal Rules of Civil Procedure (“FRCP”).¹ The definition of “relevant” is broad; evidence may be considered relevant, for example, if it can *lead* to the discovery of admissible evi-

dence.² Extensive and detailed pleadings are generally not necessary under U.S. notice pleading rules, in part because of the liberal and expansive pre-trial-discovery tools that are available to U.S. litigants and allow them to identify relevant facts and witnesses. In practice, requests for information are carried out by written interrogatories (i.e. written questions to the opposite party), judicial discovery orders, or requests for the production of documents or things (i.e. a request brought forward to a litigant by another party’s lawyer to prepare and present relevant documents). Significantly, according to Rule 34 of the FRCP, it is clear that electronically stored information (“ESI”) is governed by pre-trial-discovery regulations in the same manner as documentary evidence.³ This means that a company’s electronic information system (its servers, hard drives, back up systems, software document management systems and third party document retention systems) is also subject to discovery.⁴

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

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

2. Duty to Preserve

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

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

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

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

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

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

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